



**RÉPUBLIQUE
FRANÇAISE**

*Liberté
Égalité
Fraternité*

Les évolutions de la carte Vitale et la carte Vitale biométrique

AVRIL 2023

François **AUVIGNE**
Hadrien **HADDAK**
Adrien **BAYLE**

Carole **LÉPINE**
Vincent **RUOL**

IGF

INSPECTION GÉNÉRALE DES FINANCES



INSPECTION GÉNÉRALE
DES AFFAIRES SOCIALES

INSPECTION GÉNÉRALE DES
FINANCES
N° 2022-M-056-04

INSPECTION GÉNÉRALE DES
AFFAIRES SOCIALES
N° 2022-087R

RAPPORT

LES ÉVOLUTIONS DE LA CARTE VITALE ET LA CARTE VITALE BIOMÉTRIQUE

Établi par

HADRIEN HADDAK
Inspecteur des
finances

ADRIEN BAYLE
Inspecteur des
Finances

Sous la supervision de
FRANÇOIS AUVIGNE
Inspecteur général des
finances

CAROLE LÉPINE
Inspectrice générale des
affaires sociales

VINCENT RUOL
Inspecteur général des
affaires sociales

- AVRIL 2023 -

SYNTHÈSE

Par lettre du 18 octobre 2022, les Inspections générales des finances et des affaires sociales ont été chargées par les Ministres chargés de la santé et de la prévention et délégué aux comptes publics d'évaluer la faisabilité de la mise en œuvre d'une carte Vitale biométrique.

S'agissant de l'assurance maladie, le régime général a détecté des préjudices frauduleux à hauteur de 250 M€ à 300 M€ par an, soit environ 0,1 % des prestations servies. Toutefois, ces montants n'indiquent pas l'amplitude réelle de la fraude, qui ne peut être qu'estimée. Les derniers travaux conduits par le régime général, à ce stade uniquement dans quelques compartiments de dépenses, laissent penser qu'elle s'établirait à un niveau très supérieur, entre 3 % et 5 % des prestations servies en fonction des méthodes d'extrapolation.

La fraude détectée aujourd'hui est le fait des professionnels et établissements de santé pour environ les trois quarts des montants détectés, les assurés représentant environ un quart des montants frauduleux détectés. Au sein de la fraude du fait des assurés, les deux principaux postes de préjudice identifiés sont la fraude aux indemnités journalières et la fraude aux conditions de ressources qui permettent l'accès à la complémentaire santé solidaire et donc à une prise en charge intégrale des frais de santé. La fraude à l'usurpation d'identité, qui est précisément celle qu'une carte Vitale biométrique pourrait mettre en échec, est résiduelle en nombre de cas détectés (moins d'une dizaine par an) et en montant (quelques millions d'euros). La plupart des autres cas de fraude liée à l'usage de cartes Vitale identifiés par la mission ne serait pas ou de façon limitée empêchée par la mise en place d'une carte Vitale biométrique.

La mission propose quelques pistes non biométriques afin d'améliorer l'efficacité de la lutte contre la fraude : horodatage des flux SESAM-Vitale, prescription de médicaments onéreux ou stupéfiants sécurisée, contrôles bloquants pour les actes et dispensations aberrants, contrôles resserrés des conditions de résidence pour l'ouverture des droits à l'assurance maladie.

Pour autant, la carte Vitale est aujourd'hui la pierre angulaire d'un robuste système de facturation des soins de ville dématérialisé, fiable, au coût maîtrisé. Son usage permet de fluidifier la gestion des flux concernant les soins des assurés sociaux (les personnes non affiliées à l'assurance maladie, au premier chef les personnes relevant de l'aide médicale d'État, ne disposent pas d'une carte Vitale).

S'il est vrai que plusieurs millions de cartes Vitale dites « surnuméraires » existaient au début des années 2010, la situation est en passe d'être normalisée, sous la double action :

- ◆ structurelle, de la gestion réellement interrégimes du parc de cartes Vitale, avec notamment la possibilité de « muter » une carte Vitale, c'est-à-dire qu'une personne conserve sa carte Vitale – et n'a plus besoin de s'en faire éditer une nouvelle – lorsqu'il change de régime depuis 2010 ;
- ◆ conjoncturelle, des opérations d'apurement des bases et des mises en fin de vie massives opérées à la fin des années 2010.

Rapport

La mission a également, comme l'y invitait la lettre de mission, procédé à une évaluation de l'application carte Vitale (ApCV), qui est une version dématérialisée de la carte Vitale, qui n'a pas vocation à s'y substituer mais à compléter l'offre de service aux assurés. Si le développement des fonctionnalités prévues (délégation à un tiers ; authentification de l'identité afin d'accéder à des services numériques en santé comme Mon Espace Santé) doit être encouragé, plusieurs points demeurent à améliorer. Ainsi l'enrôlement biométrique à distance (c'est-à-dire l'inscription de l'assuré social dans le système informatique) s'avère à ce stade difficile à mettre en œuvre. L'utilisation par l'application du téléservice ADRI, permet de connaître en temps réel les droits d'un assuré et représente une réelle amélioration, en sécurisant les flux électroniques (moins de rejets en raison de droits n'étant pas à jour) et en permettant aux professionnels de santé de connaître en temps réel les droits du patient, sous la triple condition néanmoins de fiabiliser l'infrastructure, ses données et sa disponibilité. La question d'asseoir la garantie de paiement dont bénéficient les professionnels de santé sur les droits ADRI plutôt que sur les droits inscrits en carte Vitale mérite d'être sérieusement investiguée. En conclusion, si l'ApCV est un projet qui doit être soutenu, la mission préconise d'en desserrer le calendrier afin de corriger les défauts opérationnels apparus lors de la présérie – sur des échantillons très modestes – testée depuis septembre 2022.

S'agissant de la mise en œuvre d'une technologie biométrique dans la carte Vitale, la mission alerte sur le risque juridique majeur qu'elle comporterait : si les gains apportés en termes de lutte contre la fraude apparaissent très limités, la proportionnalité du traitement biométrique pourrait être difficile à établir. Surtout, dans le cas particulier de l'accès aux soins, le recours à cette technologie emporterait des inconvénients majeurs :

- ◆ exclusion d'une partie des assurés légitimes, ce qui pourrait concerner plusieurs centaines de milliers de personnes s'agissant d'un système concernant presque l'ensemble de la population française, n'arrivant pas à s'enrôler (c'est-à-dire inscrire en carte ou dans un système centralisé leurs caractéristiques biométriques) ou non reconnues par le système, entraînant un traitement manuel, donc plus lent et plus onéreux, de leur cas particulier ;
- ◆ adaptations nécessaires, par exemple en pharmacie d'officine, afin de gérer les cas légitimes où le patient n'est pas physiquement présent et ne peut s'authentifier ;
- ◆ risque de compromission des données biométriques, par nature non révocables, d'autant plus critique dans l'hypothèse où les caractéristiques biométriques seraient stockées dans un système centralisé ;
- ◆ acceptabilité très faible par les professionnels de santé qui craignent notamment une hausse des incivilités lors de leur exercice professionnel en cas de contrôle biométrique du patient ;
- ◆ complication des circuits de préadmission en établissement de santé, alors que les chantiers de dématérialisation en cours visent à les fluidifier davantage et à simplifier l'accès aux soins pour le patient.

La mission a instruit deux scénarios d'évolution biométrique, qui ont suscité l'opposition de la CNIL, en retenant deux techniques biométriques matures technologiquement et les mieux acceptées socialement : l'empreinte digitale et la reconnaissance faciale. La mission a écarté l'hypothèse d'une base centralisée, trop complexe et onéreuse à sécuriser, pour retenir celle d'une biométrie sur carte. Dans les deux hypothèses, les caractéristiques biométriques doivent être régulièrement mises à jour (nouvel enrôlement en face-à-face) pour éviter une dégradation des performances du système : tous les 10 ans pour la reconnaissance faciale, tous les 5 ans pour les empreintes digitales. Ces opérations représentent l'essentiel du coût de la mise en œuvre des solutions biométriques, estimé à au moins 1 Md€. Ces opérations entraîneraient également des désagréments pour les assurés, qui devraient se déplacer dans les organismes locaux de sécurité sociale afin de se faire enrôler.

Rapport

Enfin, la mission a exploré la possibilité d'inscrire le numéro de sécurité sociale (NIR) sur la carte nationale d'identité électronique (CNIe) ou les titres de séjour, ces titres d'identité remplaçant la carte Vitale physique qui aurait ainsi vocation à disparaître progressivement. Le NIR serait inscrit sur la puce électronique que ces titres d'identité contiennent, dans un container étanche et sécurisé, accessible uniquement par l'assurance maladie et les professionnels de santé. Ce scénario présente l'avantage d'être cohérent avec le déploiement de l'ApCV, qui prévoit l'équipement des professionnels de santé en lecteurs de puces NFC, technologie également embarquée dans la CNIe. Ce scénario, qui a suscité l'intérêt des professionnels de santé, a une double visée : la lutte contre la fraude, en sécurisant l'identité des personnes se présentant à l'occasion des soins ; la protection de la santé publique, en permettant une avancée majeure en termes d'identitovigilance, afin de sécuriser l'identité du patient et donc des données devant être portées dans son dossier médical. En première approche, la CNIL a indiqué que la mise en place de ce scénario suppose qu'un motif d'intérêt public important le justifie et mentionne plusieurs prérequis impératifs. Pour approfondir cette option, une étude de faisabilité technique et d'opportunité détaillée est à conduire par les ministères chargés de l'Intérieur et de la Santé.

En conclusion, la mission :

- ◆ recommande d'intensifier les efforts en matière de lutte contre la fraude aux prestations d'assurance maladie ;
- ◆ préconise de sécuriser le déploiement de l'ApCV, au besoin en desserrant son calendrier de généralisation ;
- ◆ ne recommande pas la mise en œuvre d'une solution biométrique, onéreuse et inadaptée au système de soins français ;
- ◆ suggère d'instruire le scénario de substitution de la carte Vitale physique par un titre d'identité régalien sur lequel serait inscrit, de manière sécurisée, le numéro d'assuré social (NIR).

SOMMAIRE

INTRODUCTION.....	1
1. LA FRAUDE AUX PRESTATIONS D'ASSURANCE MALADIE, UN SUJET DONT LA PRISE EN COMPTE EST CROISSANTE, EST LE FAIT PRINCIPALEMENT DES PROFESSIONNELS ET ÉTABLISSEMENTS DE SANTÉ	2
1.1. Les préjudices frauduleux détectés au détriment de l'assurance maladie représentaient entre 250 et 300 M€ mais pourraient être plus importants	2
1.2. La fraude des assurés représente environ un quart des montants de fraude détectés par l'assurance maladie.....	3
1.3. La fraude à l'identité ne représente probablement qu'une faible part des fraudes dans lesquelles une carte Vitale est utilisée.....	6
1.4. Quelques pistes non biométriques pourraient être explorées afin de lutter contre les cas de fraude mettant en jeu l'utilisation d'une carte Vitale	8
2. LE SYSTÈME DE LA CARTE VITALE PHYSIQUE QUI A FAIT LA PREUVE DE SA ROBUSTESSE ET DE SA PRATICITÉ, À UN COÛT DE GESTION AUJOURD'HUI MAÎTRISÉ, GAGNERA À ÊTRE DÉMATÉRIALISÉ SUR SMARTPHONE	9
2.1. La carte Vitale est la pierre angulaire d'un robuste système de facturation dématérialisée, assortie d'une garantie de paiement pour les professionnels de santé	9
2.2. La problématique des cartes surnuméraires est désormais bien documentée et le risque d'une utilisation frauduleuse massive est dorénavant maîtrisé.....	10
2.2.1. <i>A la fin de l'année 2018, il était dénombré 2,35 millions de cartes Vitale « surnuméraires ».....</i>	<i>10</i>
2.2.2. <i>A partir de 2016 des opérations de mise en fin de vie des cartes Vitale surnuméraires ont été conduites.....</i>	<i>11</i>
2.2.3. <i>Des mesures automatiques et de sécurisation mises en place protègent dorénavant les régimes d'assurance maladie de préjudices financiers liés à l'utilisation de cartes surnuméraires</i>	<i>13</i>
2.3. La carte Vitale physique présente un certain nombre de limites dans son utilisation au quotidien.....	14
2.3.1. <i>La carte Vitale présente des droits en carte non nécessairement à jour emportant, du fait de la garantie de paiement, de potentiels préjudices financiers pour l'Assurance maladie.</i>	<i>14</i>
2.3.2. <i>A l'hôpital, la carte Vitale n'est plus centrale dans les démarches d'admission en soins programmés.....</i>	<i>16</i>
2.3.3. <i>Une autre difficulté de gestion récurrente concerne les modalités de rattachement des mineurs à l'AMO et à l'AMC.....</i>	<i>16</i>
2.3.4. <i>La carte Vitale ne remplit pas les exigences de l'identitovigilance</i>	<i>17</i>
2.4. La future application carte Vitale (ApCV) constitue un réel progrès qu'il importe de déployer plus progressivement pour garantir son adoption large par les assurés.....	17
2.4.1. <i>Le projet d'application carte Vitale, lancé en 2016, propose une solution dématérialisée novatrice en termes de services et d'architecture.....</i>	<i>17</i>

2.4.2.	<i>Un enrôlement biométrique est prévu pour activer l'application et garantir la cohérence entre l'identité de l'assuré social et l'utilisateur du smartphone</i>	18
2.4.3.	<i>L'assurance maladie ambitionne une adoption large à terme de l'ApCV.</i>	19
2.4.4.	<i>Des expérimentations ont été conduites depuis 2019, et surtout à partir de septembre 2022, pour mieux définir le projet et préparer le lancement à destination du public de l'application.</i>	19
2.4.5.	<i>A court terme, une généralisation réussie de l'application carte Vitale devrait s'appuyer sur un déploiement plus progressif.</i>	20
2.4.6.	<i>A plus long terme, il faudra s'interroger sur l'articulation entre le support physique et l'application carte Vitale, en particulier sur l'avenir de la carte physique dans l'éventualité où l'adoption de l'application serait très large.</i>	21

3. OUTRE DES RISQUES JURIDIQUES ET TECHNOLOGIQUES, LE DÉPLOIEMENT D'UN SCÉNARIO BIOMÉTRIQUE SERAIT ONÉREUX ET MAL ACCUEILLI PAR LES PROFESSIONNELS ET ÉTABLISSEMENTS DE SANTÉ 23

3.1.	<i>L'usage à grande échelle de la biométrie, qui ne permet de traiter que les fraudes à l'identité, n'apparaît pas proportionné au regard du nombre de fraudes qui seraient évitées</i>	23
3.2.	<i>Les risques associés à la mise en œuvre d'une technologie biométrique à l'échelle d'une population entière sont disproportionnés par rapport à l'objectif de fiabilisation de la facturation des frais de santé.</i>	24
3.2.1.	<i>Peu de retours d'expérience à l'échelle d'une population entière sont disponibles</i>	24
3.2.2.	<i>Le recours à une technologie probabiliste entraîne des risques intrinsèques significatifs.</i>	25
3.2.3.	<i>Le risque de compromission des données aurait des conséquences néfastes durables sur la prise en charge des assurés concernés s'il se réalisait.</i>	26
3.3.	<i>La mise en place d'une carte Vitale biométrique serait coûteuse et opérationnellement complexe</i>	27
3.3.1.	<i>Les contraintes juridiques et techniques conduisent à écarter la mise en place d'une base centralisée</i>	27
3.3.1.	<i>Le recueil des données biométriques de l'ensemble des assurés sociaux devrait être effectué aux guichets des organismes de sécurité sociale.</i>	29
3.3.2.	<i>L'enrôlement de l'ensemble des assurés dans un système biométrique par empreintes digitales sur 5 ans coûterait de l'ordre de 1,2 Md€ au moins.</i>	30
3.3.1.	<i>Le déploiement d'un système biométrique par reconnaissance faciale sur 10 ans s'établirait au moins à 965 M€.</i>	31
3.3.2.	<i>Certains coûts et risques supplémentaires doivent également être pris en compte</i>	32
3.4.	<i>L'usage de la biométrie fait l'objet des plus vives réticences de la part des professionnels de santé, qu'ils exercent en ville ou en établissement.</i>	33
3.4.1.	<i>Les professionnels de santé libéraux critiquent l'inutilité de la mesure et insistent sur les risques associés.</i>	33
3.4.2.	<i>Pour les professionnels exerçant en établissement, l'usurpation d'identité est un problème de santé publique limité qui n'empêche pas la délivrance du soin.</i>	34
3.5.	<i>La CNIL n'est pas favorable aux scénarios biométriques présentés</i>	35

4. UNE SOLUTION ALTERNATIVE À LA BIOMÉTRIE EST ENVISAGEABLE : LA CNIE ET LES TITRES DE SÉJOUR POURRAIENT PORTER LE NIR DE L'ASSURÉ.....	35
4.1. Cette solution, cohérente avec la stratégie développée par les pouvoirs publics en matière de santé et d'e-santé poursuit plusieurs finalités d'intérêt général .	35
4.2. Le déploiement opérationnel sera progressif et articulé avec le calendrier de généralisation de l'application carte Vitale.....	37
4.3. En première approche, les éléments avancés par la CNIL ne sont pas bloquants.....	38

INTRODUCTION

Le ministre de la santé et de la prévention et le ministre délégué chargé des comptes publics ont, par lettre du 18 octobre 2022, chargé l'Inspection générale des finances (IGF) et l'Inspection générale des affaires sociales (IGAS) d'une mission sur la faisabilité de la mise en place d'une carte Vitale biométrique.

Cette mission s'inscrit dans le cadre de la mise en œuvre de la loi de finances rectificative n°2022-1157 du 16 août 2022 qui a ouvert une enveloppe de 20 millions d'euros au sein de la mission « santé » pour initier le chantier de la carte Vitale biométrique.

Les analyses de la fraude à la carte européenne d'assurance maladie, de la fraude à l'aide médicale d'Etat (AME), dont les bénéficiaires se voient attribuer une carte spécifique différente de la carte Vitale, et du processus d'affiliation à l'assurance maladie ont été exclues du champ de la mission.

Afin d'appréhender les modalités et l'ampleur de la fraude sociale liée à l'usage des cartes Vitale, la mission a retenu le périmètre du régime général de l'assurance maladie, excluant les autres régimes d'assurance maladie obligatoire (AMO) et l'ensemble des régimes d'assurance maladie complémentaire (AMC).

1. La fraude aux prestations d'assurance maladie, un sujet dont la prise en compte est croissante, est le fait principalement des professionnels et établissements de santé

La lutte contre la fraude aux prestations sociales, qui porte atteinte au principe de solidarité et à la légitimité des prélèvements sociaux, est une exigence de valeur constitutionnelle¹.

Depuis deux décennies, l'assurance maladie a renforcé sa politique de lutte contre la fraude, passant de 13 M€ de fraudes détectées en 2005 à 287 M€ en 2019 (1.1). Néanmoins, de nouveaux outils statistiques permettent d'évaluer la fraude réelle, qui n'émane que minoritairement des assurés, et qui est sensiblement plus élevée (1.2). L'usurpation d'identité par l'usage frauduleux de cartes Vitale ne représente qu'une part très minoritaire de la fraude émanant des assurés (1.3).

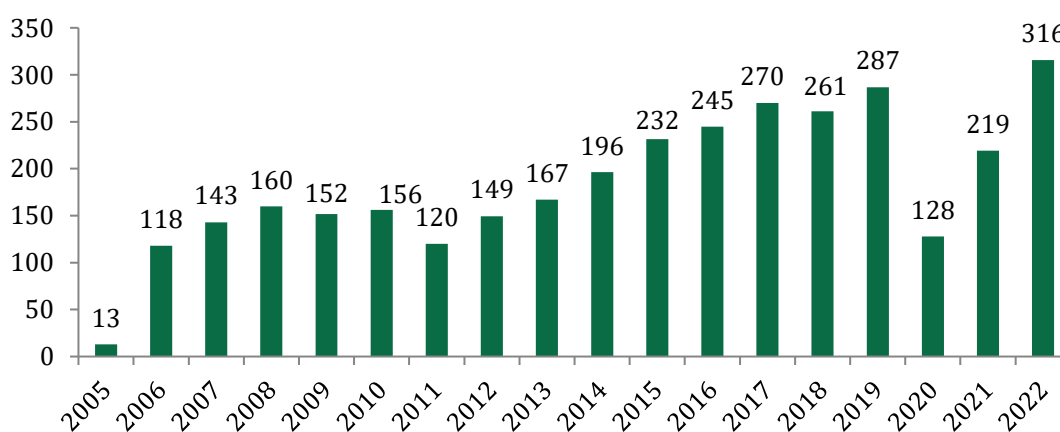
1.1. Les préjudices frauduleux détectés au détriment de l'assurance maladie représentaient entre 250 et 300 M€ mais pourraient être plus importants

La lutte contre la fraude (LCF) à l'assurance maladie s'inscrit dans un dispositif plus large d'actions d'accompagnement et de contrôle visant à s'assurer de la bonne attribution des droits, du paiement à bon droit des prestations, des remboursements de soins aux assurés et des règlements de factures aux professionnels de santé.

La lutte contre la fraude s'est renforcée en **2017** au travers d'une évolution de la stratégie élaborée par la Caisse nationale d'assurance maladie (CNAM) qui s'est concrétisée par la mise en place des premiers **plans régionaux de LCF, à compter de 2018**, puis avec le déploiement du **programme de rénovation de la gestion du risque « Rénov'GDR »**, au sein de la COG 2018-2022.

Depuis 2005, les montants de fraudes et activités fautives détectées et stoppées ont fortement augmenté chaque année à partir de 2015 (cf. graphique 1)

Graphique 1 : Montant de fraude et activité détectées et stoppées entre 2005 et 2022, régime général (en millions d'euros)



Source : CNAM, mission.

¹ Décision n° 2010-622-DC du 28 décembre 2010. Le Conseil Constitutionnel a reconnu le caractère d'une exigence constitutionnelle à la lutte contre la fraude, cette dernière allant à l'encontre de l'impératif d'efficacité économique et de juste dépense sociale.

Rapport

Les **montants des préjudices frauduleux et fautifs, subis et évités, détectés ont été croissants au début de la COG CNAM 2018-2022 (261 M€ en 2018 et 287M€ en 2019), puis ont diminué en 2020 (128 M€)**. En 2020 et 2021, la crise sanitaire a conduit à un recul des montants de fraude détectée et stoppée, notamment du fait de l'interruption des contrôles T2A dans les établissements de santé (51,8 M€ en 2019, 7,9M€ en 2020 et aucun contrôle T2A en 2021). La réduction des montants détectés s'est accompagnée d'une révision à la baisse des objectifs annuels pour ces deux exercices.

En ordre de grandeur, ces montants représentent 0,1 % des dépenses effectuées chaque année au titre de l'Assurance maladie qui sont passés de 208 Mds € en 2019 à 226 Mds€ en 2020². Les montants de fraude **détectée** sont donc très faibles au regard des montants versés.

Plusieurs éléments peuvent être avancés³ pour expliquer cet ordre de grandeur limité, notamment :

- ◆ des effectifs limités en nombre, et notamment en nombre de personnels agréés, dans les organismes locaux ;
- ◆ un outillage améliorable, en particulier en matière de *data mining* et de ciblage des contrôles ;
- ◆ des contrôles essentiellement réalisés *a posteriori* dans un système de paiement dont l'objectif premier est d'assurer un remboursement rapide des frais de santé.

Certains contrôles embarqués, comme par exemple le blocage de dispensations multiples de médicaments onéreux à un même assuré social dans un laps de temps resserré, font d'autant plus défaut que le recouvrement s'avère difficile une fois la fraude détectée. De ce point de vue, l'objectif de lutte contre la fraude peut apparaître en contradiction avec celui de fluidification des flux de facturation.

1.2. La fraude des assurés représente environ un quart des montants de fraude détectés par l'assurance maladie

Les montants de fraude détectée confirment les observations effectuées par exemple aux États-Unis⁴ qui établissent que la fraude est d'abord le fait des professionnels exerçant en ville ou d'établissements de santé.

Pour le régime général, en 2021, les principaux cas de fraude, tels que décrits par l'Assurance maladie, sont **en montant** :

- ◆ **pour environ un quart, la fraude provenant des assurés sociaux** :
 - dispensation, au moyen de fausses ordonnances, puis revente de médicaments onéreux ou stupéfiants, dans le cadre d'organisations criminelles ;
 - indemnités journalières (IJ) perçues à tort, ce type de fraude nécessitant l'intervention d'un professionnel de santé (prescription médicale) ;

² Charges nettes de la CNAM. Source : Rapport au ministère chargé de la Sécurité sociale et au Parlement sur l'évolution des charges et des produits de l'Assurance Maladie au titre de 2023 (loi du 13 août 2004).

³ Voir notamment, pour le régime général, le rapport de l'IGAS n° 2022-027 d'évaluation de la COG2018-2022 de la CNAM et recommandations en vue de son renouvellement, janvier 2023.

⁴Health Care Fraud; October 27, 2009;S. ROSENBAUM, N. LOPEZ, S. STIFFLER; George Washington University, School of Public Health and Health Services, Department of Health Policy : « *Estimates are that 80% of healthcare fraud is committed by medical providers, 10% by consumers, and the balance by others, such as insurers themselves and their employees* ». Le contexte de prise en charge est toutefois très différent de celui existant en France.

Rapport

- il convient d'ajouter, même si les montants détectés par le régime général sont moindres, les fraudes à l'affiliation (condition de résidence) et les fraudes aux conditions de ressources (qui permettent une meilleure prise en charge financière dans le cadre de la complémentaire santé solidaire – C2S) ;
- ◆ **pour environ trois quarts, la fraude provenant des professionnels de santé, liée à la surfacturation d'actes ou à la facturation d'actes fictifs.**

Afin d'évaluer l'ampleur de la fraude et de s'appuyer sur ces données pour améliorer l'efficacité de son action, la CNAM a réalisé, à compter de novembre 2020, un travail de **comparaison des méthodes d'estimation de la fraude qui ont été employées en France** (par les autres branches du régime général et les autres régimes, Pôle Emploi, la CCMSA, l'INSEE) **et en Europe.**

Ces travaux ont montré l'intérêt du recours aux **méthodes de post stratification ou économétrique afin d'extrapoler, sur la base de la fraude détecté par les contrôles réalisés, des montants estimés de fraude**⁵.

Depuis 2021, ces travaux ont été conduits dans différents compartiments de dépenses, à ce stade, pour certaines professions de santé et quelques dispositifs comme la C2S.

Sur les compartiments de dépenses de l'Assurance maladie où ces techniques ont ainsi été déployées, il apparaît que la **fraude estimée** est substantiellement supérieure à la fraude détectée (cf. tableau 1) et avoisinerait **3 % à 5 % des montants remboursés.**

⁵ Cf. Annexe III.

Rapport

Tableau 1 : Évaluation de l'ampleur de la fraude estimée et comparaison par rapport à la fraude détectée (données 2019)

Profession de santé contrôlée	Montants totaux remboursés (en M€)	Montants préjudices financiers (en M€)	Taux de préjudice financier détecté	Extrapolation brute		Extrapolation statistique (post-stratification ou matching)	
				Montants préjudices financiers extrapolés (en M€)	Taux de préjudice financier	Montants préjudices financiers extrapolés (en M€)	Taux de préjudice financier
Infirmiers libéraux (IDEL) *	5 700	17,8	0,3 %	339	5,9 %	286	5,0 %
Médecins généralistes	6 000	4	0,1 %	256	4,3 %	185	3,1 %
Transporteurs	3 600	12,3	0,3 %	182	5,1 %	177	4,9 %
Pharmaciens	17 500	11,3	0,1 %	151	0,9 %	105	0,6 %
Masseurs-kinésithérapeutes	3 200	4,7	0,1 %	245	7,6 %	166	5,2 %

1.3. La fraude à l'identité ne représente probablement qu'une faible part des fraudes dans lesquelles une carte Vitale est utilisée

Toute personne affiliée à la sécurité sociale peut demander l'établissement d'une carte Vitale personnelle dès 16 ans⁶ – et peut en obtenir une entre 12 ans et 16 ans mais à l'initiative de ses représentants légaux. La **détention d'une carte Vitale n'est pas obligatoire⁷ et n'est pas émise systématiquement**. Un assuré social peut par exemple faire valoir ses droits en produisant une attestation sous forme papier.

La carte d'assurance maladie ou carte Vitale est un **support électronique personnalisé et interrégimes** diffusé à partir de 1998 auprès de l'ensemble des assurés sociaux, tous régimes confondus, par le GIE SESAM-Vitale, qui remplit des objectifs multiples. Elle constitue :

- ◆ un **support de l'identité de l'assuré** et celles des ayants-droit⁸. Cette identité est fondée sur le numéro d'inscription au répertoire (NIR) communément appelé numéro de sécurité sociale ;
- ◆ un **support des droits ouverts auprès des régimes d'assurance maladie obligatoire (AMO)**, facilitant leur exercice pour l'obtention de remboursements ou d'avances de frais sur des prestations de santé ; les droits inscrits en carte doivent faire l'objet d'une mise à jour une fois l'an⁹ ;
- ◆ un **outil de signature électronique qui sécurise les flux électroniques de facturation** et permet le remboursement des frais de santé sous une semaine sans avoir besoin d'envoyer à l'Assurance maladie une feuille de soins papier. Les services de lutte contre la fraude des caisses primaires d'assurance maladie (CPAM) et de la CNAM rencontrés par la mission remarquent d'ailleurs que les fraudes détectées sont en proportion supérieures parmi les flux non sécurisés de facturation, c'est-à-dire ceux établis en l'absence de carte Vitale.

Si la carte Vitale peut être utilisée dans certaines fraudes, elle n'en est que dans quelques cas le vecteur unique, pouvant être remplacée de manière simple par une attestation de droits papier.

La fraude liée à l'usage des cartes ne constitue ainsi pas une catégorie opérante permettant aux équipes de lutte contre la fraude des régimes d'assurance maladie de déployer des contre-mesures d'ordre général.

La mission propose, dans le but d'analyser l'impact d'un traitement biométrique sur la fraude à l'usage des cartes, une liste des principaux cas de fraudes aux prestations d'assurance maladie pouvant mettre en jeu un usage de la carte Vitale (cf. tableau 2).

⁶ Entre 16 et 18 ans existe la possibilité d'être soit un assuré de droit direct, soit l'ayant droit de ses parents (CSS, art. L. 160-2).

⁷ CSS, article L. 161-33.

⁸ Personne qui tient son droit à l'assurance maladie-maternité du fait de ses liens avec un assuré de plus de 16 ans.

⁹ Article R161-33-10 du code de la sécurité sociale.

Rapport

Tableau 2 : Récapitulatif des principaux cas de fraude « avec carte Vitale »

Type de fraude	Modalité de la fraude	Portée de la fraude
Usurpation d'identité (assurés)	Utilisation frauduleuse d'une carte Vitale perdue ou volée	Accès aux prestations de santé
	Fraude au tiers-payant au moyen de la carte Vitale d'un assuré en bénéficiant	Prise en charge financière (ALD, C2S, etc.)
	Utilisation de la carte Vitale d'un tiers par une personne en situation irrégulière non éligible à l'aide médicale d'État (AME)	Accès aux prestations de santé et, selon les droits, prise en charge financière
	Utilisation de la carte Vitale d'un tiers par une personne ayant des droits ouverts mais en recherche d'anonymat (grossesses non désirées, maladies sexuellement transmissibles)	Impact financier limité Erreur dans les informations renseignées au dossier médical
Fraude à la condition de résidence (assurés)	Ouverture de droits, et accès à une carte Vitale, au bénéfice d'une personne qui ne justifie pas d'un séjour régulier lui permettant d'être éligible à la protection universelle maladie (PUMA)	Accès aux prestations de santé et, selon les droits, prise en charge financière
	Maintien de l'accès aux soins malgré le non-respect de la condition de résidence stable en France pour des personnes ayant déjà bénéficié de la PUMA à bon droit, qui conservent et utilisent leur carte Vitale	Accès aux prestations de santé et, selon les droits, prise en charge financière
Fraude à la délivrance de médicaments (assurés)	Utilisation de fausses prescriptions pour obtenir frauduleusement la délivrance de médicaments onéreux ou stupéfiants ; l'assuré, en général titulaire de droits ouverts, se présente en officine avec sa carte Vitale	Prise en charge financière (médicaments onéreux) Alimentation du trafic de produits stupéfiants
Professionnels de santé	Facturation d'actes fictifs en utilisant la carte Vitale d'un patient ou l'empreinte de carte Vitale conservée dans le logiciel de facturation	Prise en charge financière
	Facturation d'actes plus coûteux que ceux effectivement réalisés (sur-cotation) en utilisant la carte Vitale d'un patient ou l'empreinte de carte Vitale conservée dans le logiciel de facturation	Prise en charge financière

Source : Mission.

Dans cette liste, seule la fraude à l'usurpation d'identité – et, pour partie, la facturation de certains actes fictifs – est mise en échec, en théorie, par l'usage de la biométrie (cf. 3.1). Or, s'il n'est pas possible d'évaluer les montants financiers en jeu dans ce type de fraude, deux éléments conduisent à les supposer peu significatifs :

- ◆ d'une part, les cas d'usurpation d'identité ou de fraude à l'identité représentaient des montants très faibles, quoique croissants, pour l'assurance maladie¹⁰ : 3,2 M€ de préjudices détectés en 2022 contre, en 2021, 2,4 M€ et en 2020, 1,5 M€ ;

Rapport

- ◆ d'autre part, les professionnels et établissements de santé rencontrés par la mission, s'ils confirment l'existence d'une fraude à l'identité de patients, insistent sur son caractère résiduel : quelques cas constatés sur l'ensemble d'une carrière de praticien libéral, ou moins d'une dizaine de cas chaque année pour des établissements de santé situés dans une zone où les patients présentent des situations sociales fragiles.

Au surplus, il n'est pas certain que ces usurpations d'identité entraînent systématiquement un préjudice financier pour les administrations publiques. En effet, si l'usurpation d'identité de la part d'une personne dépourvue de droits existe bien, les cas types décrits par les praticiens regroupent également des situations dans lesquelles des droits existeraient :

- ◆ lorsque le patient usurpant est citoyen français et pourrait se voir ouvrir des droits à l'assurance maladie dans le cadre de la protection universelle maladie (PUMa), mais y renonce en raison de sa distance au système de sécurité sociale¹¹ ;
- ◆ lorsque le patient usurpant est un travailleur irrégulier, il remplit en toute vraisemblance les conditions d'ouverture de droits à l'AME.

Il convient également de signaler les cas d'usurpations d'identité n'ayant pas de conséquences financières :

- ◆ afin de garantir l'anonymat, notamment en santé sexuelle ;
- ◆ afin d'obtenir des avantages non financiers (comme le passe sanitaire lorsqu'il était en vigueur ou un titre de séjour pour soins en usurpant une pathologie).

1.4. Quelques pistes non biométriques pourraient être explorées afin de lutter contre les cas de fraude mettant en jeu l'utilisation d'une carte Vitale

Certaines mesures, bien que non expertisées par la mission, pourraient être envisagées en réponse à la typologie proposée *supra* :

- ◆ un horodatage des flux SESAM-Vitale permettrait de contrôler certaines cotations frauduleuses ou actes fictifs ;
- ◆ des contrôles embarqués dans les systèmes d'information et bloquants avant la facturation, en particulier en matière de dispensation de médicaments onéreux, permettraient d'arrêter plus vite certaines fraudes ;
- ◆ le déploiement de la e-prescription est une mesure attendue afin de mettre en échec la fraude à la délivrance de médicaments ;
- ◆ les contrôles PUMa, sur les ressources mais également sur l'affiliation à raison de la résidence, gagneraient à être plus fréquents et serrés (notamment s'agissant des documents justificatifs) ;
- ◆ enfin, l'usage de DOCVERIF afin de s'assurer de la validité de titres d'identité français (y compris les titres de séjour) pourrait intéresser les organismes de base (lors de l'affiliation) mais surtout les établissements de santé (lors de la phase d'admission pour les soins programmés).

¹⁰ Source : bilans 2019, 2020 et 2021 de la politique de lutte contre la fraude et les activités fautives établi par l'assurance maladie conformément à l'article L.114-9 du code de la Sécurité sociale.

¹¹ Le cas des gens du voyage a été particulièrement signalé à la mission par les praticiens rencontrés.

2. Le système de la carte Vitale physique qui a fait la preuve de sa robustesse et de sa praticité, à un coût de gestion aujourd'hui maîtrisé, gagnera à être dématérialisé sur smartphone

2.1. La carte Vitale est la pierre angulaire d'un robuste système de facturation dématérialisée, assortie d'une garantie de paiement pour les professionnels de santé

Le parc de cartes Vitale, qui s'établit à 57,9 millions de cartes valides au 31 décembre 2021, est renouvelé à hauteur d'environ 4 millions de cartes émises chaque année. La mission n'a pas étudié en détail la qualité de service perçue par les assurés en matière de délivrance de la carte. Le coût complet de gestion et de production d'une carte Vitale actuelle est maîtrisé à 4,33 € l'unité¹² ce qui conduit à estimer à environ 17 M€ le coût annuel de renouvellement du parc.

Historiquement, les feuilles de soin étaient transmises aux régimes d'assurance maladie sous format papier. **La carte Vitale a constitué l'élément central de la politique de développement de la feuille de soins électronique (FSE)**, de sa transmission dématérialisée aux régimes d'assurance maladie obligatoire et complémentaire (cf. encadré 1).

Avec un taux de dématérialisation de près de 95 % des feuilles de soins en 2020, le chantier de la dématérialisation est quasiment achevé, porté par la garantie de paiement accordée aux professionnels de santé¹³, qui leur garantit le paiement des actes sur la base des informations inscrites dans la carte Vitale du patient et ce, même si elles ne sont pas à jour.

L'émission de FSE a permis aux régimes d'assurance maladie de réaliser d'importants gains de productivité, et donc des économies¹⁴, tout en accélérant les remboursements aux assurés et les paiements aux professionnels de santé opérés aujourd'hui sous sept jours ouvrés¹⁵.

Encadré 1 : Typologie des FSE

Parmi les flux de feuilles de soins électroniques, on trouve notamment :

les flux sécurisés SESAM Vitale, co-signés conjointement par la carte Vitale et par la carte du professionnel de santé, qui représentent **72% des FSE transmises en 2022**¹⁶ ; ces flux bénéficient de la garantie de paiement ;

les flux sécurisés SESAM sans Vitale, pour certains actes médicaux spécifiques (biologie, santé sexuelle des mineurs, téléconsultation) et envoyés en l'absence de la carte Vitale du patient, qui représentent **13 % des FSE en 2022** ; ces flux bénéficient de la garantie de paiement

les flux SESAM Vitale dégradé, dit flux B2, un mode de transmission alternatif au mode sécurisé et permettant de créer une FSE en l'absence de carte Vitale du patient, qui représentent **15% des FSE en 2022** ; le professionnel de santé doit également transmettre une feuille de soins papier revêtue de la signature du patient afin d'attester de la présence de ce dernier ; ces flux ne bénéficient pas de la garantie de paiement.

¹² Source : GIE SESAME Vitale et CNAM, cf. annexe VI.

¹³ Renforcée en 2016 à l'occasion de la généralisation du tiers payant.

¹⁴ Alors que le coût de traitement d'une FSE s'établirait à 0,27 € contre 1,74 € pour une feuille de soins papier (source GIE SESAM-Vitale).

¹⁵ Article D.161-13-3 du code de la sécurité sociale.

¹⁶ Période de 12 mois allant de décembre 2021 (inclus) à novembre 2022 (inclus), données GIE-SESAM-Vitale.

2.2. La problématique des cartes surnuméraires est désormais bien documentée et le risque d'une utilisation frauduleuse massive est dorénavant maîtrisé

2.2.1. À la fin de l'année 2018, il était dénombré 2,35 millions de cartes Vitale « surnuméraires »

La détention d'une carte Vitale ne constituant pas une obligation, il n'y a **pas de lien automatique entre le nombre d'assurés affiliés à l'assurance maladie et le nombre de cartes Vitale valides** en circulation.

Un régime d'assurance maladie présente des cartes Vitale en surnombre, phénomène identifié par plusieurs rapports en 2019 et en 2020, lorsque **l'ensemble des cartes Vitale valides dépasse le nombre de personnes affiliées à ce régime. La notion de cartes Vitale « surnuméraires »** correspond donc à un **solde**, au niveau d'un régime ou à un niveau agrégé tous régimes confondus.

Des défauts dans la gestion initiale du parc de cartes et, pendant plusieurs années, une mauvaise communication entre régimes d'assurance maladie ont conduit au fil du temps à une accumulation de cartes surnuméraires.

Les cartes Vitale surnuméraires sont celles qui n'ont pas été invalidées alors que l'assuré :

- ◆ n'a plus de droits ouverts (cas plus restreints en pratique depuis la mise en œuvre de la PUMa en 2016) suite à un changement de situation ou à son décès ;
- ◆ a changé de régime ou a perdu (ou s'est fait voler) sa carte et s'est vu délivrer une nouvelle carte Vitale.

Malgré l'absence d'obligation de détention d'une carte Vitale, les différents régimes d'assurance maladie ont accumulé au fil des ans des excédents de cartes, pour atteindre **un montant cumulé de 2,35 millions de cartes surnuméraires à la fin de l'année 2018** (cf. tableau 3).

Une des raisons principales de l'accumulation de ce stock est qu'**avant 2010, aucun système n'inscrivait les cartes surnuméraires issues d'une perte ou d'un changement de régime en liste d'opposition**. La double délivrance de carte était donc possible pour un même assuré avant cette date et avant la création, également en 2010, d'un portail SI interrégimes permettant de bloquer la délivrance d'une nouvelle carte dès lors que l'ancienne était toujours en circulation¹⁷.

¹⁷ Cf. Annexe II.

Rapport

Tableau 3 : Comparaison entre le nombre d'assurés sociaux de plus de 16 ans et le nombre de cartes Vitale valides par régime au 31 décembre 2018

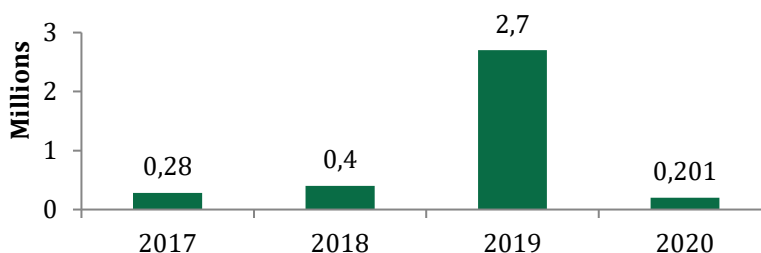
Régime	Assurés de 16 ans et plus ¹⁸	Cartes Vitale valides ¹⁹	Cartes Vitale surnuméraires	Cartes valides/Assurés de 16 ans et plus
01- Régime Général	45 163 570	43 367 835	-	96 %
02- Régime Agricole – MSA	2 790 220	3 141 869	351 649	113 %
03- S.S.I.	3 872 483	4 479 689	607 206	116 %
04- S.N.C.F	393 389	465 818	72 429	118 %
05- R.A.T.P	85 836	101 752	15 916	119 %
06- ENIM (Marine)	88 996	96 306	7 310	108 %
07- Mines	107 339	162 431	55 092	151 %
08- Militaires de Carrière	668 095	768 886	100 791	115 %
10- Clercs, Employés de Notaire	94 626	119 505	24 879	126 %
14- Assemblée Nationale	4 849	5 100	251	105 %
15- Sénat	3 450	4 207	757	122 %
90- C.A.V.I.M.A.C. (cultes)	42 209	97 529	55 320	231 %
91- M.G.E.N	2 551 751	2 520 351	-	99 %
92- Mutuelle des PTT	6 869	147 357	140 488	N.S.
93- Mutuelle Générale Police	124 432	184 333	59 901	148 %
94- Fédér. Fonctionnaires (SLI)	821 833	840 395	18 562	102 %
95- M.N.H.	248 894	294 264	45 370	118 %
96- Harmonie Fonction Publique	162 161	167 893	5 732	104 %
99- Autres Mutuelles	1 678 936	2 470 516	791 580	147 %
Total	58 909 938	59 436 036	2 353 233	-

Source : CNAM.

2.2.2. A partir de 2016 des opérations de mise en fin de vie des cartes Vitale surnuméraires ont été conduites

Les régimes d'assurance maladie obligatoire procèdent depuis 2016 à des opérations de mise en fin de vie des cartes Vitale en doublon ou dont les titulaires n'ont plus de droits ou sont décédés ou radiés (cf. graphique 2). Ces cartes mises en fin de vie dans le système sont placées automatiquement en **liste d'opposition**.

Graphique 2 : Cartes mises en liste d'opposition par le régime général suite à des campagnes ciblées entre 2017 et 2020 (en millions)



Source : GIE SESAM Vitale.

L'inscription en liste d'opposition préserve les régimes d'assurance maladie du risque de préjudice financier (cf. encadré 2).

¹⁸ Source : RNIAM.

¹⁹ Source : GIE SESAM-Vitale.

Encadré 2 : Liste d'opposition, facturation et garantie de paiement

Depuis 2004 : la mise en place de **listes d'opposition** empêche toute facturation à l'assurance maladie à partir des cartes Vitale qui y sont inscrites.

En complément, pour l'ensemble des professionnels de santé, le **téléservice de consultation des droits des assurés en ligne ADRI** (acquisition des droits intégrée) **utilisé avec une carte Vitale dans le lecteur fait un contrôle d'opposition de la carte** ce qui permet à chaque profession d'avoir accès à la liste d'opposition ;

Enfin, les contrôles de liste d'opposition sont également faits dans les **centraux des assurances maladie lors du traitement des FSE avec** :

- en cas de paiement vers l'assuré pour un flux hors tiers payant, un signalement déclenchant un contrôle systématique et un processus de récupération de la carte ;
- pour un flux en tiers payant avec garantie de paiement, un signalement au professionnel de santé.

Les cartes invalidées, permettent au professionnel de santé de **télétransmettre les FSE**. Le cas échéant, les règlements dus aux professionnels de santé sont honorés (**garantie de paiement associé à l'usage de la carte Vitale**). Cela explique qu'une partie des flux engendrés par ces cartes ont suscité des paiements. Inversement, les **règlements à l'assuré sont rejetés** avec un code rejet spécifique.

En 2019, **330 000 feuilles de soins ont été concernées, soit 0,023 % des feuilles de soins électroniques (FSE)**. Pour plus des deux tiers, le règlement a été stoppé. Pour le tiers restant, soit environ 100 000 feuilles de soins adressées dans le cadre d'un tiers payant réalisé par un professionnel de santé, la CNAM a réglé à hauteur de 4 millions d'euros au titre de la garantie de paiement (applicable dès lors qu'une carte Vitale est utilisée).

Les campagnes d'apurement, menées ces dernières années et permettant de mettre en fin de vie un grand nombre de cartes surnuméraires, arrivent à leur terme.

Les dernières statistiques de septembre 2022 font état de **949 cartes surnuméraires pour l'ensemble des régimes** (cf. tableau 4). Elles se répartissent entre :

- ◆ 706 cartes pour le régime des mines²⁰ ;
- ◆ 226 cartes pour le régime de l'Assemblée nationale ;
- ◆ 17 cartes pour le régime du Sénat.

²⁰ Au 31 décembre 2022, le régime ne comptabilisait déjà plus de carte surnuméraire.

Rapport

Tableau 4 : Comparaison entre le nombre d'assurés sociaux de plus de 16 ans et le nombre de cartes Vitale valides par régime au 30 septembre 2022

Régime	Assurés de 16 ans et plus	Cartes Vitale valides.	Cartes Vitale surnuméraires	Cartes valides/Assurés de 16 ans et plus
01- Régime Général et absorbés	52 991 881	50 803 527	-	96 %
02- Régime Agricole – MSA	2 726 269	2 723 952	-	100 %
04- S.N.C.F	346 132	343 018	-	99 %
05- R.A.T.P	84 861	82 728	-	97 %
06- ENIM (Marine)	80 270	77 060	-	96 %
07- Mines	81 241	81 947	706	101 %
08- Militaires de Carrière	661 868	632 061	-	95 %
10- Clercs, Employés de Notaire	108 585	106 905	-	98 %
14- Assemblée Nationale	4 923	5 149	226	105 %
15- Sénat	3 530	3 547	17	100 %
90- C.A.V.I.M.A.C. (cultes)	41 773	36 219	-	87 %
91- M.G.E.N	2 610 919	2 552 284	-	98 %
93- Mutuelle Générale Police	118 448	116 714	-	99 %
99- Régime 99	449 366	432 584	-	96 %
Tous régimes	60 310 066	57 997 695	949	-

Source : CNAM.

2.2.3. Des mesures automatiques et de sécurisation mises en place protègent dorénavant les régimes d'assurance maladie de préjudices financiers liés à l'utilisation de cartes surnuméraires

L'inscription automatique en liste d'opposition depuis 2019 de toutes les cartes Vitale en doublon car remplacées après un cas de perte ou vol, du fait de changement de régime, de la fermeture des droits ou du décès de l'assuré **empêche, à l'avenir, la reconstitution d'un stock de cartes surnuméraires.**

Au niveau de chaque régime néanmoins, le solde constaté peut masquer des situations de compensation en l'absence de données plus précises sur le nombre exact d'assurés de 16 ans et plus non porteurs d'une carte Vitale. Les assurés de moins de 20 ans sont en effet moins porteurs de carte Vitale, la transition du statut d'ayant droits à un statut de porteur d'une carte Vitale à part entière pouvant prendre quelque temps. Des assurés de 16 ans et plus peuvent ne pas être équipés de carte Vitale et théoriquement compenser des cartes Vitale excédentaires attribuées à d'autres assurés. Des cartes surnuméraires peuvent donc potentiellement subsister pour des régimes qui présentent, en solde, une situation réglée.

Dans le cas du régime général, en particulier investigué par la mission²¹, les données consultées (notamment par classes d'âge) montrent que le régime ne présente plus, hors un stock frictionnel réduit, de situation de cartes Vitale en surnombre. Il est suggéré que des vérifications équivalentes soient effectuées par les autres régimes d'assurance maladie afin d'aboutir à des conclusions plus complètes sur les cartes surnuméraires, en particulier :

- ◆ l'identification des assurés non porteurs de cartes Vitale ;
- ◆ le dénombrement des détenteurs de cartes Vitale par tranche d'âge.

²¹ Cf. Annexe II.

Rapport

S'agissant du risque financier, il est à noter tout d'abord qu'une carte surnuméraire n'est pas nécessairement « consommante », c'est à dire générant de frais de santé. Il n'est pas possible de se prononcer sur les niveaux de consommation de soins des cartes surnuméraires auparavant mises en fin de vie du fait d'une absence de données - dont la durée de conservation trop courte (deux ans pour les données de santé les plus fines) aura conduit à leur suppression avant le lancement de la présente mission.

Si, toutefois, une carte surnuméraire était à nouveau utilisée, il existe des éléments de maîtrise de risque dans le système qui préservent les régimes d'assurance maladie de préjudices financiers substantiels :

- ◆ lorsqu'une carte Vitale est émise ou mise à jour, une « date de fin de droits » (correspondant à la date de personnalisation ou de mise à jour à laquelle est ajoutée un an) est inscrite en carte pour chaque bénéficiaire. Un professionnel de santé recevant un assuré avec une carte avec des droits échus refusera *a priori* le tiers payant et demandera un paiement direct ;
- ◆ dans le cas où la carte surnuméraire n'a pas été invalidée, où les droits ne sont pas échus et où une facturation est effectuée, elle est identifiée dans les systèmes d'information des régimes d'assurance maladie et est inscrite en liste d'opposition²².

En tout état de cause, l'usage d'une carte Vitale surnuméraire n'a pas engendré dans les quelques cas étudiés de remboursements *a priori* injustifiés de la part de l'assurance maladie.

Dans le cas spécifique du régime du Sénat, en particulier investigué, il apparaît par exemple qu'aucune consommation sur les 678 cartes surnuméraires identifiées n'avait été constatée en 2021. D'après la CNAM, en 2019, les montants déboursés par le régime général au titre d'un flux généré par une carte Vitale surnuméraire n'ont pas bénéficié à des personnes dépourvues de droits. Par conséquent, dans le cas d'espèce, le préjudice est nul ou du moins négligeable.

2.3. La carte Vitale physique présente un certain nombre de limites dans son utilisation au quotidien

2.3.1. La carte Vitale présente des droits en carte non nécessairement à jour emportant, du fait de la garantie de paiement, de potentiels préjudices financiers pour l'Assurance maladie.

La carte Vitale contient les informations relatives au détenteur et à ses droits. Ces données étant inscrites sur la puce de la carte, elles peuvent ne plus être à jour en cas de changement de situation de l'assuré social (déménagement, ALD, changement de médecin traitant, changement d'organisme assurant la prise en charge des frais de santé, etc.).

Afin de limiter les écarts entre les droits ouverts et ceux portés par la carte Vitale, il est prévu une **obligation de mise à jour annuelle ou lors d'un changement de situation personnelle**. Cette mise à jour est à effectuer en pharmacie ou sur les bornes mises à disposition dans les caisses primaires d'assurance maladie.

²² Dans un délai qui peut varier si une saisie manuelle en caisse locale est nécessaire. Pour une description plus fine des processus en caisse primaire, voir le rapport de l'IGAS n° 2022-084, Contrôle de la CPAM de la Haute-Marne.

Rapport

En pratique, cette opération est effectuée en moyenne 1,2 fois par an – le plus souvent à l'initiative des pharmaciens²³, mais 20 % des cartes valides n'avaient pas été mises à jour en 2021 ne serait-ce qu'une seule fois dans l'année²⁴. Les droits ainsi contenus en carte ne sont donc pas nécessairement à jour lorsqu'il en fait la présentation au professionnel de santé pour la facturation d'un acte (cf. tableau 5).

Tableau 5 : Nombre de cartes valides sans mise à jour depuis plus de deux ans

Délai de non mise à jour	Nombre de cartes Vitale valides
Sans télémise à jour depuis 6 ans	128 985
Sans télémise à jour depuis 5 ans	194 866
Sans télémise à jour depuis 4 ans	303 014
Sans télémise à jour depuis 3 ans	539 254
Sans télémise à jour depuis 2 ans	1 074 058

Source : GIE SESAM-Vitale d'après les données de décembre 2022 ; cartes Vitale émises avant 2022 et valides au 30 novembre 2022.

Or, que les droits en carte aient été ou non actualisés, les professionnels de santé bénéficient d'**une garantie de paiement des droits inscrits sur la puce**. Cela peut amener les régimes d'assurance maladie à supporter un préjudice financier dont le montant est potentiellement important mais que l'assurance maladie n'est pas en mesure d'évaluer précisément.

Depuis 2015, la CNAM a développé le **téléservice ADRI** à destination des professionnels de santé exerçant en ville, actualisé quotidiennement et qui permet de parer à l'absence de mise à jour automatique des droits inscrits sur la carte Vitale.

Ce téléservice, intégré aux logiciels de facturation, permet, en temps réel, de consulter les droits d'un assuré social, quel que soit son régime d'appartenance et d'éviter les rejets de facturation liées aux écarts entre les droits de la carte Vitale et les droits de la base de l'Assurance Maladie.

Le recours au téléservice conduit à une réduction sensible du taux de rejet, tous flux de facturation confondus (dégradés ou non dégradés), et en particulier **de diviser par deux le taux de rejet des factures réalisées avec une carte Vitale**.

Le recours à ADRI a été en hausse rapide depuis 2015. Les appels au téléservice s'élevaient en 2022 à plus de 743 millions d'appels sur les onze premiers mois de l'année, soit dix fois plus qu'en 2018 et près de deux fois plus qu'en 2020. Le taux de FSE réalisé avec ADRI s'établissait à 24,7 % en moyenne en 2022, soit un quart du nombre total des FSE annuelles émises²⁵.

La mission estime que la généralisation du téléservice ADRI devrait être résolument encouragée.

²³ Qui disposent du matériel nécessaire en lecture / écriture (soit environ 100 000 terminaux) pour modifier les données stockées sur la carte Vitale, contrairement aux autres professionnels de santé (sauf exceptions).

²⁴ Source : GIE SESAM Vitale, 2021-CMS VITALE TOUS REGIMES.

²⁵ Source : CNAM. Données établies à partir des données figurant dans le tableau de bord de suivi d'ADRI de novembre 2022.

2.3.2. A l'hôpital, la carte Vitale n'est plus centrale dans les démarches d'admission en soins programmés

Un téléservice équivalent (CDRi²⁶) a été développé spécifiquement pour les logiciels de facturation des établissements de santé, qui ne sont pas facturés à l'acte. Il permet de restituer les droits à jour du patient et d'intégrer les données des droits automatiquement dans leur logiciel de gestion administrative. A fin novembre 2022, il était utilisé par 81 % des établissements FIDES et 15 % des établissements sanitaires hors FIDES²⁷.

Dans ces établissements, lors de l'admission dans le cadre de soins programmés, la carte Vitale n'est plus consultée que pour restituer le NIR des patients, et non plus pour vérifier l'existence et la nature des droits ouverts. En 2022, le GIE SESAM-Vitale fait état de 70 millions d'appels CDRi, en hausse constante, et de 316 millions de consultations à CDR²⁸.

2.3.3. Une autre difficulté de gestion récurrente concerne les modalités de rattachement des mineurs à l'AMO et à l'AMC

Actuellement, un enfant de moins de 16 ans est rattaché à sa naissance en qualité d'ayant droit à la carte Vitale d'un des deux parents, le plus souvent à celle de sa mère. Il peut également être rattaché à la carte Vitale des deux parents à leur demande, tout en conservant un rattachement « principal »²⁹ à l'une des deux cartes.

Le rattachement d'un enfant mineur à la carte de l'un ou des deux parents génère des difficultés spécifiques et récurrentes de plusieurs ordres :

- ◆ un frein à l'accès aux soins et à la prise en charge des frais de santé lorsqu'un mineur se présente seul au cabinet du médecin ou qu'il réside chez un tiers, en cas de garde par les grands parents par exemple ;
- ◆ des difficultés de remboursement des frais de santé rapportées par les caisses primaires et les organismes d'assurance maladie complémentaires interrogés, ou en officine (lorsque le mineur attend pendant plusieurs semaines sa carte Vitale personnelle, ou en cas de rejet de facturation lorsque les cartes des deux parents ne sont pas mises à jour simultanément), à plus forte raison lorsque les parents sont séparés notamment en cas d'avance de frais.

Si ce mode de gestion des enfants mineurs devait être conservé, la mission suggère que le rattachement aux cartes Vitale des deux parents soit opéré dès la naissance de manière systématique de manière à favoriser une égale prise en charge des enfants par les deux parents.

²⁶ Consultation des droits intégrée (CDRi).

²⁷ Source : CNAM. Le service FIDES (Facturation Individuelle Des Établissements de Santé) permet de facturer individuellement et directement les actes et consultations externes du domaine MCO (médecine, chirurgie, obstétrique et odontologie) aux caisses d'assurance maladie.

²⁸ Téléservice accessible en ligne et qui n'est pas intégré au logiciel de facturation.

²⁹ Pour l'envoi des courriers de l'assurance maladie qui concernent l'enfant mineur.

2.3.4. La carte Vitale ne remplit pas les exigences de l'identitovigilance

Pour les professionnels de santé comme pour les établissements, fiabiliser l'identification des usagers est une obligation déontologique et une nécessité médicale pour s'assurer que les soins sont délivrés au bon patient avant d'être un enjeu de bon usage des finances publiques³⁰.

Les procédures d'identitovigilance³¹, qui ont été renforcées pour les professionnels de santé depuis la mise en place du référentiel 'identifiant national de santé' (INS) supposent donc de s'assurer, *a minima* lors du premier contact physique de l'utilisateur dans une structure, que les justificatifs d'identité présentés correspondent bien à la personne prise en charge.

Les dispositifs ou documents acceptés sont les dispositifs d'identification électroniques apportant un niveau de garantie substantiel ou élevé au sens du règlement européen eIDAS³², ou des titres régaliens d'identité. La carte Vitale ne permet pas de qualifier l'INS, alors même que cette étape est devenue un élément clé de qualité et de sécurité des soins.

En établissement, une pièce d'identité est demandée systématiquement lors de l'admission : carte Vitale et titre d'identité sont présentés de manière conjointe ou séparée – le patient ayant tendance à davantage oublier sa carte Vitale que sa pièce d'identité³³.

En ville, demander une pièce d'identité pour pouvoir qualifier l'INS d'un patient³⁴ et référencer les données de santé dans son dossier médical ne fait pas partie des habitudes des praticiens, qui pour une partie d'entre eux s'y refusent.

2.4. La future application carte Vitale (ApCV) constitue un réel progrès qu'il importe de déployer plus progressivement pour garantir son adoption large par les assurés

2.4.1. Le projet d'application carte Vitale, lancé en 2016, propose une solution dématérialisée novatrice en termes de services et d'architecture

L'application est porteuse d'avancées majeures pour toutes les parties prenantes :

- ◆ pour les usagers :
 - l'application offre la possibilité de disposer d'une **version dématérialisée de sa carte Vitale sur son smartphone**, sur un mode similaire aux produits développés par le secteur bancaire ;

³⁰ Font partie « [des] exigences de valeur constitutionnelle » celles « qui s'attachent tant à la protection de la santé, qui implique la coordination des soins et la prévention des prescriptions inutiles ou dangereuses, qu'à l'équilibre financier de la sécurité sociale » d'après la décision du conseil constitutionnel n° 2004-504 DC du 12 août 2004.

³¹ L'identitovigilance est l'ensemble des mesures mises en œuvre pour fiabiliser l'identification de l'utilisateur afin de sécuriser ses données de santé, à toutes les étapes de sa prise en charge.

³² Le règlement n° 910/2014/UE sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, dit règlement « eIDAS », établit un socle commun pour les interactions électroniques sécurisées entre les citoyens, les entreprises et les autorités publiques.

³³ Dans le cas d'étude de la mission au service des admissions de l'hôpital universitaire Avicenne.

³⁴ Une fois qualifiée par le professionnel de santé ou l'établissement, l'INS est vérifiée par un appel au téléservice INSi.

Rapport

- l'application offrira également une fonction de **portefeuille d'identités** (le NIR, l'identité d'assuré à une complémentaire santé, l'INS et les traits d'identité civile) et une fonction de **fourniture d'une identité numérique** d'un niveau de sécurité suffisant **pour l'accès sécurisé des assurés aux services numériques de l'assurance maladie ou de la santé** (notamment à Mon Espace Santé) ;
- à la différence de la carte Vitale physique, les usagers pourront avec l'application consulter leurs dépenses de soins ou déléguer à un tiers de confiance – disposant également de l'application – leur carte Vitale dématérialisée de façon encadrée et traçable ;
- ◆ pour les professionnels et les établissements de santé :
 - l'application carte Vitale est une solution dématérialisée facilitant les actes de facturation : le professionnel n'aura plus à manipuler la carte physique de l'assuré, qui par la présentation d'un QR code ou d'une puce NFC³⁵ permettra l'appel de ses droits pour la facturation ;
 - au-delà du gain de temps, l'ApCV s'articule efficacement avec l'INS et Mon espace santé. En établissement de santé, l'application pourra notamment contribuer à faciliter les démarches de préadmissions en soins programmés réalisées à distance ;
- ◆ pour les régimes d'assurance maladie :
 - l'application appelle systématiquement, pour la facturation, les droits renseignés dans ADRI, donc les droits à jour, remédiant ainsi à une lacune structurelle majeure de l'architecture locale de la carte physique. L'application carte Vitale, par l'appel aux bases de droits ouverts en temps réel, devrait ainsi permettre aux régimes d'assurance maladie d'éviter certains préjudices financiers constatés dans les cas d'utilisation de cartes Vitale non à jour ;
 - l'application permet une facturation sécurisée, y compris dans les situations de téléconsultations.

2.4.2. Un enrôlement biométrique est prévu pour activer l'application et garantir la cohérence entre l'identité de l'assuré social et l'utilisateur du smartphone

L'application carte Vitale comprend un enrôlement biométrique par reconnaissance faciale pour attester l'identité de la personne ayant téléchargé l'application. Cette fonctionnalité vise à s'assurer que le titulaire de l'application carte Vitale est bien celui qu'il prétend être. Elle n'a pas pour but de vérifier l'identité de la personne à chaque usage de l'application.

L'enrôlement biométrique est aussi une condition de sécurisation pour que l'ApCV, à la différence de la carte Vitale physique, soit utilisée pour s'identifier électroniquement à d'autres services numériques de santé.

Concrètement, l'assuré doit prendre une vidéo de lui-même (*selfie*). Cette vidéo est ensuite automatiquement analysée pour vérifier la conformité entre la photographie de la pièce d'identité et le visage capté en flux vidéo, tout en s'assurant qu'il s'agit bien d'une personne réelle et d'une pièce d'identité valide. En cas de résultat positif des opérations biométriques par algorithme, l'ensemble est enfin validé par un opérateur humain sous deux jours ouvrables.

³⁵ Near Field Communication.

2.4.3. L'assurance maladie ambitionne une adoption large à terme de l'ApCV

Le taux de pénétration des smartphones dans la population étant de l'ordre de 75 % à 85 % avec néanmoins d'importantes disparités entre classes d'âge, il ouvre des perspectives favorables d'équipement de la population générale en cartes Vitale dématérialisées, avec l'ambition d'une couverture large à moyen terme.

La coexistence sur longue période des deux supports, physique et dématérialisé, est une nécessité, en sus du maintien de l'attestation de droits papier³⁶. Le téléchargement de l'application reposera sur une base volontaire. L'application carte Vitale ne sera ainsi pas obligatoire.

Les assurés, qu'ils soient ou non équipés en smartphone, conserveront le choix du support permettant de justifier leurs droits. Ce dernier point a notamment été accueilli favorablement par la CNIL³⁷.

2.4.4. Des expérimentations ont été conduites depuis 2019, et surtout à partir de septembre 2022, pour mieux définir le projet et préparer le lancement à destination du public de l'application

Une première expérimentation a été lancée en septembre 2019 afin d'observer l'utilisation de l'application carte Vitale dans la vie de tous les jours : facilité de l'installation sur le smartphone et de la prise en main, ergonomie, cas réels d'usage, pertinence des technologies mises en œuvre, identification des freins.

Le champ géographique de cette expérimentation était très restreint. Seuls deux organismes du régime général (CPAM Rhône et CPAM Alpes-Maritimes) et deux organismes de la MSA (Ain-Rhône et Provence-Azur) ont été intégrés à l'expérimentation.

Le processus d'enrôlement de cette première expérimentation s'appuyait sur une **vérification d'identité à distance sans inclure de traitement biométrique**. L'assuré devait envoyer des photographies de sa pièce d'identité et de son visage, sans mise en place d'un flux vidéo.

A la fin du mois d'août 2022, cette expérimentation comptabilisait **114 professionnels de santé équipés**. Le test n'a pas été réalisé en établissement de santé. Du côté des utilisateurs, **6 430 assurés avaient activé l'application carte Vitale** sur leur smartphone. Au cours de cette expérimentation, seules **157 feuilles de soin électroniques ont été établies**.

Les choix faits ont conduit à une première expérimentation réduite sur le plan quantitatif, qui a également pâti des conséquences de la crise sanitaire. Néanmoins, les enquêtes qualitatives réalisées auprès des utilisateurs *a posteriori*, ont confirmé l'intérêt des cas d'usage identifiés pour l'application, le bénéfice d'avoir des droits pour la facturation à jour, l'avantage d'une utilisation sans contact.

Une seconde expérimentation, conduite à partir de septembre 2022 dans la perspective d'une ouverture au public d'une application cible, a permis de **tester au travers d'une présérie l'enrôlement biométrique et le fonctionnement des flux de facturation**.

³⁶ Téléchargeable en ligne, à partir du compte ameli de l'assuré.

³⁷ Délibération n° 2022-097 du 8 septembre 2022 de la CNIL (JORF du 30 décembre 2022).

Rapport

La présérie n'a été testée que sur un nombre limité d'assurés familiarisés avec les nouvelles technologies, auprès des agents du GIE SESAM-Vitale et des agents des CPAM de 8 départements³⁸. **561 activations avaient été initiées sur Android.** La volumétrie des tests s'est également révélée faible, avec **51 feuilles de soins électroniques réalisées en 44 rendez-vous entre le 19 septembre et le 21 octobre 2022.**

Cette présérie ne s'est pas avérée immédiatement opérationnelle pour une diffusion à un plus large public. Elle a montré la **nécessité d'améliorer les performances en particulier de la phase d'activation initiale de l'application carte Vitale.** Seules 34,5% des activations sont réussies sans rencontrer d'erreur lors de l'étape du flux vidéo. **L'échec à l'activation s'élève au demeurant à 35,5 % des activations initiées.** Les parcours d'enrôlement ont en effet été impactés par une instabilité des flux vidéo et un paramétrage élevé en termes de sécurité. A la date de la mission, des corrections étaient en cours pour améliorer l'expérience utilisateur.

Par ailleurs, la mission ne peut se prononcer sur la capacité de cette application cible testée depuis septembre 2022 et sur l'architecture cible, à tenir une charge sensiblement plus élevée en cas de déploiement large.

Ces deux phases de test, en raison de leur volumétrie très faible, ne permettent pas de conclure au fonctionnement opérationnel de l'application à grande échelle si elle venait à être rapidement généralisée.

Sans attendre les bilans définitifs des expérimentations conduites, **la décision d'une généralisation a été prise.** Le décret n° 2022-1719 du 28 décembre 2022 relatif aux moyens d'identification électronique interrégimes, en effet, permet la généralisation de l'application carte Vitale et l'extension des services proposés.

Le calendrier a néanmoins connu d'importants décalages. La présérie, en test entre septembre 2022 et février 2023, devait par exemple être initialement testée en 2021 puis a été décalée à juin 2022 avant de se tenir finalement en septembre 2022.

Le lancement à destination des assurés des huit départements identifiés devait avoir initialement lieu à la fin de l'automne 2022. Il a plutôt été fait le choix, en septembre 2022, au vu des premiers résultats de la présérie de décaler cette ouverture. Dans le nouveau calendrier, l'ouverture plus large aux assurés, département par département, ou région par région, pourrait débuter courant 2023.

2.4.5. A court terme, une généralisation réussie de l'application carte Vitale devrait s'appuyer sur un déploiement plus progressif

L'application carte Vitale rejoint une demande de dématérialisation exprimée par les assurés comme par les professionnels de santé. Les résultats des études qualitatives menées dans le cadre des expérimentations confirment l'aspect novateur de la solution et ses avantages comparativement à la traditionnelle carte physique. Plusieurs pays européens ont mis en place de tels applicatifs (notamment le Danemark, l'Allemagne, le Portugal³⁹).

La généralisation de l'ApCV, et sa diffusion à un grand nombre d'assurés, apparaît donc comme souhaitable et porteuse d'avancées majeures dans la modernisation du système de santé.

³⁸ Le Rhône (69), les Alpes Maritimes (06), la Sarthe (72), la Loire-Atlantique (44), le Puy de Dôme (63), le Bas Rhin (67), la Saône et Loire (71), la Seine Maritime (76).

³⁹ cf. Annexe VIII.

Rapport

Toutefois, la faible volumétrie et le nombre réduits de participants aux expérimentations, fruit des choix méthodologiques effectués, ont conduit à constater tardivement dans le processus de développement de la présérie des difficultés techniques et opérationnelles appelant de multiples corrections.

Un déploiement trop rapide d'une application présentant encore trop de dysfonctionnements, dont certains particulièrement problématiques comme par exemple lors de la phase d'activation, ferait porter un risque réputationnel à l'ApCV qui concentrerait les critiques virulentes des premiers usagers, pouvant dissuader d'autres de procéder à un téléchargement.

Pour que la généralisation de l'application carte Vitale soit réussie, il semble donc qu'une plus grande progressivité dans son déploiement soit à rechercher, avec un calendrier desserré et un effort particulier porté en 2023 à l'apport de corrections techniques.

Un délai supplémentaire serait également utile pour équiper davantage de professionnels de santé de matériels compatibles pour la facturation avec l'application, condition essentielle d'une généralisation réussie. Dans cet intervalle de temps, le bilan de la deuxième expérimentation pourrait être consolidé et présenté à la CNIL. Du reste, la CNAM mène en parallèle des travaux visant à sécuriser la fiabilité de l'infrastructure supportant le téléservice ADRI et dont le fonctionnement à une charge substantiellement supérieure est crucial pour le développement concomitant de l'application carte Vitale.

2.4.6. A plus long terme, il faudra s'interroger sur l'articulation entre le support physique et l'application carte Vitale, en particulier sur l'avenir de la carte physique dans l'éventualité où l'adoption de l'application serait très large

S'il sera à court terme possible de posséder les deux supports, cette situation pourrait évoluer. La généralisation de l'utilisation de l'applicatif sera une opportunité de réduire le nombre de cartes physiques – dont on peut anticiper une baisse des commandes du fait du changement de comportement de la part des usagers, et donc les coûts de gestion associés.

Dans l'immédiat, l'application apportera des éléments de sécurisation supplémentaire mais **il est incertain qu'elle permette de lutter efficacement contre la fraude**. Par ailleurs, la mise à disposition de deux supports au lieu d'un seul, à court et moyen terme, facilitera le prêt (légitime ou non) de carte physique de la part d'assurés qui, disposant de l'ApCV, n'en auront donc plus l'utilité directe⁴⁰.

À moyen terme, le fonctionnement à grande échelle d'une application qui prévoit un enrôlement biométrique conduira à interroger le développement *via* cet outil d'**une biométrie à l'usage, c'est-à-dire d'un traitement biométrique valide préalable à l'émission d'un QR code ou validant le fonctionnement d'un lien NFC lors de chaque accès aux soins**.

Cette biométrie à l'usage, comme moyen de lutter contre la fraude, **ne présente néanmoins que peu d'intérêt opérationnel et serait probablement impraticable sur le plan technique** :

- ♦ il est probable que les fraudeurs ciblés par cette mesure se déportent vers des méthodes d'attestation non biométrique de leurs droits ;
- ♦ la biométrie à l'usage sur l'ApCV n'offrirait aucune garantie supplémentaire à la sécurisation d'un usage du smartphone déjà protégé par un code ou par une ouverture biométrique ;

⁴⁰ Les questions posées par la coexistence des supports et leur articulation font l'objet de propositions de la part de la mission en fin de rapport.

Rapport

- ◆ la réutilisation des systèmes biométriques embarqués dans les smartphones est inopérante car il ne serait pas possible de s'assurer de l'intégrité du gabarit retenu dans les solutions biométriques des systèmes d'exploitation pour cette biométrie à l'usage. Par conséquent, l'Assurance maladie ne pourrait garantir que l'utilisation courante de l'application carte Vitale soit faite par le titulaire légitime du NIR déclaré ;
- ◆ enfin, les dispositifs biométriques des smartphones sont « propriétaires », c'est-à-dire à la main des entreprises propriétaires des systèmes d'exploitation, dont les performances sont très variables d'un appareil et d'une version à l'autre : s'appuyer sur ces dispositifs pourrait conduire à devoir développer une nouvelle application carte Vitale et à réécrire autant d'algorithmes de rapprochement qu'il existe de versions de systèmes d'exploitation.

3. Outre des risques juridiques et technologiques, le déploiement d'un scénario biométrique serait onéreux et mal accueilli par les professionnels et établissements de santé

3.1. L'usage à grande échelle de la biométrie, qui ne permet de traiter que les fraudes à l'identité, n'apparaît pas proportionné au regard du nombre de fraudes qui seraient évitées

Un contrôle biométrique est efficace dans un cas unique de fraude : l'usurpation d'identité⁴¹.

En effet, les principaux cas de fraude mettant en jeu l'usage d'une carte Vitale ne seraient pas mis en échec par l'adoption d'une technologie biométrique :

- ◆ fraude à l'affiliation, par exemple pour la C2S qui suppose une fraude sur la condition de ressources ou la condition de résidence ;
- ◆ fraude à la délivrance de médicaments, qui se fait aujourd'hui essentiellement sous l'identité propre d'un complice ;
- ◆ fraude aux actes facturés par les professionnels de santé, et dont un seul serait – peut-être – empêché par l'usage de la biométrie : lorsqu'une famille dispose de la C2S, il est possible que le professionnel de santé facture des actes pour l'ensemble des personnes dont les droits figurent en carte (parent et ayants-droits) et non pour la seule personne recevant les soins.

Par conséquent, la mise en place d'une carte Vitale biométrique aurait un impact probablement limité sur l'étendue des fraudes aux prestations d'assurance maladie dès lors que les usurpations d'identité représentent des montants *a priori* peu significatifs.

En établissement de santé, son déploiement n'apporterait aucun avantage relatif sérieux, étant donné que d'une part le déploiement de l'INS (dans le cadre du renforcement de l'identitovigilance) incite à une vigilance accrue dans la bonne authentification de l'identité du patient, et d'autre part que les soignants, en particulier aux urgences, prennent en charge les patients sans considération pour l'existence de droits à l'assurance maladie.

Ainsi, sur la mise en place d'un traitement biométrique, la Direction des affaires juridiques⁴² des ministères sociaux indique, au regard de l'article 9.2 du règlement général de protection des données, que « *le principe de proportionnalité, principe général applicable à l'ensemble des caractéristiques et conditions de mise en œuvre de tout traitement (les données, leur durée de conservation, leurs destinataires, leurs modalités d'accès, etc.) doit en tout état de cause être systématiquement respecté* ». Ce principe « *implique de qualifier et préciser le risque de fraude afin de vérifier si une telle comparaison est adéquate et proportionnée* ». S'agissant de l'objectif de lutte contre la fraude, la proportionnalité du traitement biométrique apparaît difficile à établir. Cela implique qu'un projet de traitement biométrique s'exposerait probablement à un risque juridique sérieux s'il avait cette seule finalité.

Quant à l'usage de la biométrie avec un objectif d'identitovigilance, qui est un objectif de santé publique, une alternative, sur laquelle sont engagés les acteurs du secteur, existe : la présentation d'une pièce d'identité probante avec une photo récente⁴³.

⁴¹ Idéalement dans l'hypothèse où le contrôle biométrique permet d'effectuer à la fois un traitement d'identification et d'authentification.

⁴² Voir annexe VII.

⁴³ La carte nationale d'identité électronique est valable 10 ans, ce qui assure qu'elle comporte une photographie d'identité relativement récente.

3.2. Les risques associés à la mise en œuvre d'une technologie biométrique à l'échelle d'une population entière sont disproportionnés par rapport à l'objectif de fiabilisation de la facturation des frais de santé

La technologie biométrique, qui est entrée dans la vie courante d'une partie des usagers avec le déblocage des smartphones, est perçue comme étant fiable par deux tiers des citoyens et jouit globalement d'une bonne image⁴⁴.

Elle présente plusieurs avantages, dont ceux d'introduire un degré de sécurité avec une simplicité d'usage et un certain confort : le « verrou biométrique » est insensible à l'oubli, à la perte, au vol, et, dans une moindre mesure au risque de copie, contrairement à d'autres facteurs d'authentification que sont les codes, les clés, ou les badges d'accès.

Toutefois elle s'avère peu utilisée à l'échelle de la population entière et présente des limites inhérentes à une technologie probabiliste qui induisent pour les usagers des risques en termes d'exclusion ou de non-recours, en cas de faux négatif lors du contrôle ou en cas de compromission des données.

3.2.1. Peu de retours d'expérience à l'échelle d'une population entière sont disponibles

L'assurance maladie n'utilise jusqu'à présent aucune donnée biométrique au cours de la production d'une carte Vitale physique. La photographie qui figure sur les cartes Vitale émises depuis 2007 ne peut être exploitée à des fins biométriques, conformément à l'avis rendu par la CNIL à l'époque. Pour les cartes qui disposent d'une telle photographie, soit deux tiers du parc actuel de cartes, celle-ci est de qualité médiocre et n'est pas actualisée⁴⁵ : son utilité est marginale, de l'avis de la quasi-totalité des professionnels de santé rencontrés qui ne la regardent que rarement.

Aucun pays développé n'a subordonné l'accès aux soins ou la prise en charge des frais de santé à un traitement biométrique préalable, à la connaissance de la mission⁴⁶. En revanche, dans plusieurs pays européens, les assurés présentent un titre d'identité lorsqu'ils se rendent chez un professionnel de santé ou en établissement de santé.

Même pour les titres sécurisés⁴⁷ détenus par la population française, on ne trouve que deux cas de contrôle biométrique :

- ◆ lors de la délivrance ou du renouvellement d'un titre sécurisé en mairie (carte d'identité et passeport) ;
- ◆ lors du passage dans les sas du système PARAFE de contrôle aux frontières dans une dizaine de points de passage à la frontière, notamment aéroportuaires⁴⁸.

⁴⁴ Cf. annexe V.

⁴⁵ Si les droits figurant sur la carte Vitale ont une durée limitée, le support physique (la carte elle-même) n'a pas d'échéance (comme c'est par exemple le cas d'une carte nationale d'identité).

⁴⁶ Cf. annexe VIII.

⁴⁷ Document officiel qui fait l'objet d'une procédure de production et de contrôle sécurisée. La gestion de production et de contrôle des titres sécurisés incombe à l'Agence Nationale des Titres Sécurisés (ANTS).

⁴⁸ Et sous réserve du consentement pour les titulaires d'un passeport électronique.

3.2.2. Le recours à une technologie probabiliste entraîne des risques intrinsèques significatifs

La technologie biométrique consiste en la comparaison :

- ◆ d'un modèle biométrique de référence, le **gabarit**, réputé décrire les caractéristiques propres à une personne (empreintes digitales, traits du visage ou de l'iris, etc.) ;
- ◆ avec les caractéristiques présentées par la personne soumise au contrôle biométrique.

Deux limites principales apparaissent alors dans le cadre de cette comparaison⁴⁹ :

- ◆ le risque de **faux positif**, c'est-à-dire d'accepter à tort un individu (l'algorithme estime à tort que le gabarit de référence et celui présenté par la personne contrôlée proviennent de la même personne). Ce risque présente une difficulté particulière par exemple quand il s'agit de restreindre l'accès à des locaux ou passer une frontière ;
- ◆ le risque de **faux négatif**, c'est-à-dire d'écarter à tort un individu (l'algorithme estime à tort que le gabarit de référence et celui présenté par la personne contrôlée proviennent de deux personnes différentes). Ce risque présente une difficulté particulière par exemple en matière d'accès aux soins, celui-ci étant légalement et même constitutionnellement protégé.

Le paramétrage du système biométrique est donc capital. Toutefois, une meilleure performance en termes de faux positifs entraîne une dégradation de la performance en termes de faux négatifs et réciproquement. Cela signifie concrètement que, dans le cas de la carte Vitale biométrique, le paramétrage devrait être calibré pour limiter le nombre de cas de faux négatifs, avec comme conséquence pratique une augmentation du nombre de cas de faux positifs et donc une limitation de l'efficacité dans la lutte contre la fraude.

Au surplus, les performances d'un même système biométrique peuvent varier⁵⁰ :

- ◆ en fonction du matériel utilisé (précision des capteurs) ;
- ◆ en fonction des logiciels d'extraction du gabarit qui peuvent différer entre le modèle vivant et le gabarit de référence ;
- ◆ en fonction des conditions d'utilisation :
 - pour la reconnaissance faciale, les conditions d'éclairage, de contraste, de luminosité, ou le fait de porter un masque par exemple peuvent faire varier les résultats ;
 - pour les empreintes digitales, la température ou l'humidité peuvent faire varier, pour une même personne, les résultats.

⁴⁹ Voir annexe V pour une description plus précise des différentes limitations et types d'erreur liés à l'usage de la technologie biométrique.

⁵⁰ Parfois même considérablement : ces dernières années, la presse britannique s'est régulièrement fait l'écho des mauvais résultats obtenus par le système de reconnaissance faciale mis en place par la police britannique avec des taux faussés dans plus de 90% des cas.

Rapport

- ◆ en fonction de l'évolution de la personne : en vieillissant ou dans le cadre de certaines pathologies, certaines mesures biométriques peuvent varier (le visage défiguré par certaines pathologies ou accidents ; des microcoupures sur les doigts liées aux activités domestiques, de loisirs ou professionnelles). La dégradation des performances est particulièrement sensible sur moyenne ou longue période : ainsi le taux de rejet du contrôle biométrique s'établit au mieux à 1 % au retrait d'un passeport⁵¹ mais à 25 % 10 ans après, lors du dépôt d'une demande de renouvellement⁵², ce qui représenterait plusieurs dizaines de milliers d'assurés sociaux si ces chiffres étaient transposés à l'échelle de l'assurance maladie. La sensibilité de la biométrie à l'évolution du vivant contraint à renouveler régulièrement le gabarit, entraînant des coûts pour le système biométrique.

Enfin, pour une partie de la population assurée, rendre obligatoire un contrôle biométrique entraînerait un risque de non-recours ou de discrimination non négligeable en matière d'accès aux soins⁵³. Ainsi en 2019, le National Institute for Standards and Technology (NIST), agence du Département du Commerce des Etats-Unis, a trouvé que la majorité de 189 algorithmes de reconnaissance faciale étudiés étaient biaisés et s'avéraient moins précis pour les populations issues de minorités ethniques et raciales. Certains interlocuteurs de la mission ont par ailleurs évoqué les difficultés à mettre en place un tel contrôle pour les enfants mineurs et les personnes majeures protégés.

3.2.3. Le risque de compromission des données aurait des conséquences néfastes durables sur la prise en charge des assurés concernés s'il se réalisait

La donnée biologique n'est pas secrète, tout individu laisse quotidiennement derrière lui des traces : empreintes digitales⁵⁴, voix (sur un répondeur par exemple), forme de son visage (sur des photographies ou des vidéos), signature, etc. Toutes les techniques biométriques, même les plus récentes sont sensibles à la contrefaçon⁵⁵ et ont été contrefaites⁵⁶.

Or, le principal désavantage du recours à un facteur d'authentification biométrique réside dans son caractère irrévocable. Ainsi, une fois la donnée biométrique corrompue⁵⁷, les données biométriques ne pourraient plus être réutilisées et il faudrait utiliser d'autres moyens d'authentification, tout en étant à la merci d'une usurpation d'identité sur une base biométrique.

Les conséquences de la compromission sont différentes dans le cas d'un système centralisé, pour lequel l'ensemble de la population en base voit ses données corrompues, ou décentralisé, où seul le porteur de carte connaît ces désagréments.

⁵¹ L'algorithme estime que les empreintes digitales au dépôt ne correspondent pas à celles du retrait.

⁵² Jusqu'à 25% constaté lors des renouvellements de passeports par l'ANTS.

⁵³ Risque évoqué de manière récurrente par le Défenseur des droits.

⁵⁴ Ce point a d'ailleurs été soulevé par le Conseil constitutionnel dans sa décision DC 2012-652 du 22 mars 2012 (considérant 10) : « les données biométriques enregistrées dans ce fichier, notamment les empreintes digitales, étant par elles-mêmes susceptibles d'être rapprochées de traces physiques laissées involontairement par la personne ou collectées à son insu, sont particulièrement sensibles ».

⁵⁵ Cf. ANSSI, « Recommandations relatives à l'authentification multifacteur et aux mots de passe », 08/10/2021.

⁵⁶ Cf. annexe V.

⁵⁷ Cf. annexe V. Les technologies biométriques dites révocables relèvent à ce stade plus de travaux de recherche que de solutions éprouvées et praticables.

Rapport

S'il n'est pas possible de garantir l'inviolabilité d'un système d'information dans le temps⁵⁸, des mesures de sécurité importantes peuvent être mises en œuvre, comme c'est par exemple le cas pour la base TES (titres électroniques sécurisés). Il n'en demeure pas moins que les bases de données biométriques constituent même des cibles de choix pour les *hackers*.

Ce risque n'est pas théorique : ces dernières années, les cas de fuites de bases de données biométriques se sont multipliés, parallèlement au recours accru à ces techniques⁵⁹. C'est la raison pour laquelle l'ANSSI recommande de ne pas utiliser un facteur d'authentification inhérent seul mais plusieurs facteurs d'authentification⁶⁰ associés à un mécanisme cryptographique conforme au référentiel général de sécurité⁶¹.

Enfin, les risques de dépendance technologique revêtent une importance particulière dans le cadre de la protection des données personnelles : le stockage de la donnée brute serait nécessaire pour permettre aux autorités de conserver la maîtrise du gabarit et leur indépendance vis-à-vis des industriels (maîtrise des algorithmes d'enrôlement et de lecture et indépendance vis-à-vis des matériels/logiciels) – ce que la CNIL ne recommande toutefois pas, préférant le stockage d'un gabarit, moins attentatoire pour les libertés individuelles.

Le recours à la technologie biométrique pour sécuriser la prise en charge des frais de santé de la population des assurés sociaux serait donc porteur d'importants risques en contrepartie d'un impact réduit sur la fraude à l'usage des cartes Vitale.

Les caractéristiques et limitations inhérentes à la technique biométrique, explorée dans les scénarios biométriques présentés *infra*, montrent au demeurant qu'elle serait complexe à mettre en œuvre et peu acceptable par les professionnels et établissements de santé.

3.3. La mise en place d'une carte Vitale biométrique serait coûteuse et opérationnellement complexe

3.3.1. Les contraintes juridiques et techniques conduisent à écarter la mise en place d'une base centralisée

La réalisation d'un traitement biométrique peut être effectuée à partir des données biométriques stockées :

- ◆ dans une base centralisée regroupant l'ensemble des gabarits biométriques des assurés sociaux ;
- ◆ dans un support individualisé, c'est à dire ne comportant que les données de son titulaire sur la puce (« *match on card* » lorsque le support est une carte équipée d'un capteur).

Ce choix joue sur la performance du dispositif, dès lors que seule une base centralisée permet de s'assurer qu'un même individu n'est pas présent plus d'une fois dans la base.

⁵⁸ Comme le rappelle l'audit ANSSI/DINSIC relatif au système TES, 17 janvier 2017, « *il est impossible de garantir l'inviolabilité absolue d'un système d'information dans le temps. La question de la sécurité (...) renvoie à l'arbitrage que doit faire l'Etat en matière d'acceptation des risques résiduels inévitables liés à la mise en œuvre de ce système, au regard des bénéfices escomptés, (...) comme c'est le cas pour tout système d'information, quelle que soit sa sensibilité* ».

⁵⁹ Exemple en 2019 de la faille de sécurité massive dans un système biométrique utilisé par les banques, la police et les entreprises de défense du Royaume-Uni, a révélé les empreintes digitales de plus d'un million de personnes.

⁶⁰ Qui ne sera pas forcément biométrique, par exemple un mot de passe, un code pin, une question secrète, ou la détention d'un appareil tels qu'un smartphone...

⁶¹ Pris en application du décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives.

Rapport

Lorsque la donnée est stockée sur la carte, seul un traitement d'authentification peut être opéré pour s'assurer que l'identité biométrique référencée sur la carte correspond à celle de son porteur (cf. graphique 3)

Graphique 3 : Schéma de traitement d'authentification



Source : GIE SESAM Vitale.

En croisant la fréquence du traitement biométrique à l'architecture retenue, on obtient des scénarios plus ou moins risqués et invasifs en termes de respect de la vie privée et plus ou moins efficaces en matière de lutte contre la fraude (cas A, B, C, D cf. tableau 6) :

Tableau 6 : Traitements biométriques possibles pour une carte Vitale biométrique selon l'architecture et la fréquence retenues

Efficacité en matière de lutte contre la fraude (de + à +++)		Fréquence du traitement biométrique	
		Uniquement à l'enrôlement lors de la création de la carte	A chaque utilisation de la carte Vitale chez un professionnel de santé
Architecture du traitement biométrique	Le gabarit biométrique est uniquement stocké sur la carte physique sur un mode décentralisé	<p style="text-align: center;">CAS A (+)</p> Un traitement est opéré à l'enrôlement uniquement ce qui permet d'authentifier que le détenteur de la carte est bien son bénéficiaire.	<p style="text-align: center;">CAS B (++)</p> Outre le traitement à l'enrôlement, un traitement d'authentification est opéré à chaque passage chez un professionnel de santé pour s'assurer que le porteur de la carte est le bénéficiaire.
	Le gabarit biométrique est stocké dans une base centralisée (éventuellement anonymisée)	<p style="text-align: center;">CAS C (+++)</p> Outre un traitement d'authentification, un traitement d'identification est opéré une fois à l'enrôlement pour vérifier qu'à une empreinte ne correspond qu'un seul individu	<p style="text-align: center;">CAS D (++++)</p> Outre le traitement d'identification à l'enrôlement, un traitement d'authentification avec recherche dans la base est opéré à chaque passage chez un professionnel de santé.

Source : Mission.

Peu de pays européens (Espagne, Pays Bas, Lituanie⁶²) ont fait le choix, comme la France, d'une base centralisée pour délivrer une carte d'identité biométrique sécurisée. La base TES (titres électroniques sécurisés), utilisée uniquement à des fins d'authentification⁶³, centralise les données recueillies lors de l'établissement d'une carte d'identité ou d'un passeport. L'accès à cette base par l'Assurance maladie est exclu, tant pour des raisons juridiques que techniques :

⁶² Cf. rapport d'information sur l'usage de la biométrie en France et en Europe n°688, établi par MM. François BONHOMME et Jean-Yves LECONTE, sénateurs, 13 juillet 2016.

⁶³ Cf. annexe V relative au recours à la biométrie

Rapport

- ◆ les mesures techniques prises pour sécuriser les données du fichier TES sont maximales : liaisons dédiées, données chiffrées, authentification forte des personnes habilitées, contingentement des connexions, consultation par lien unidirectionnel chiffré, etc. L'ouverture de cette base à un nombre important d'acteurs (professionnels et établissements de santé) n'est pas envisageable en termes de sécurité ;
- ◆ dans son courrier à la mission (cf. *infra*), la CNIL exclut l'usage par l'assurance maladie d'une base centralisée- qui nécessiterait par hypothèse des niveaux de garantie équivalents à ceux de la base TES.

Il convient donc d'exclure les scénarios C et D, les plus efficaces en termes de lutte contre la fraude.

La mission a élaboré deux scénarios biométriques « *match on card* » permettant un traitement d'authentification biométrique, à partir des deux modalités les mieux acceptées des usagers et dont les technologies matures ont été déployées à grande échelle⁶⁴ : la reconnaissance faciale et les empreintes digitales.

3.3.1. Le recueil des données biométriques de l'ensemble des assurés sociaux devrait être effectué aux guichets des organismes de sécurité sociale

La création d'une carte Vitale biométrique pose la question des conditions matérielles du recueil de la donnée biométrique pour pouvoir procéder à l'enregistrement du gabarit de son titulaire. De l'avis des experts⁶⁵, seul un enrôlement en « *face-à-face* » permet de s'assurer de l'authenticité de la donnée biométrique.

La réalisation de cette opération par les professionnels de santé ou en officine doit être écartée :

- ◆ cet enrôlement technico-administratif ne relève pas de leur compétence métier ;
- ◆ et le temps nécessaire pour procéder à cette opération ne serait donc pas consacré à leur activité médicale ou paramédicale.

La mission a également écarté l'hypothèse d'un établissement de la carte Vitale biométrique par les agents responsables de celui des titres sécurisés, qui s'appuie sur 4 100 dispositifs de recueil et remise en mairie⁶⁶. S'agissant d'un dispositif d'une volumétrie comparable, voire supérieure en cas d'enrôlement rapide de l'ensemble des assurés, une compensation devrait être versée par les régimes d'assurance maladie aux collectivités territoriales dont la charge de travail serait au moins doublée. Le contexte actuel de tensions sur la délivrance des titres d'identité régional contribue également à écarter à ce stade cette hypothèse.

Il ressort donc de ces considérations que l'enrôlement biométrique de l'ensemble de la population des assurés sociaux doit être réalisé par les agents des caisses locales de l'assurance maladie pour un coût de masse salariale chargée estimé à 535 M€ au total⁶⁷.

⁶⁴ Cf. annexe V.

⁶⁵ Pour l'ANSSI, le caractère irrévocable du facteur inhérent fait de la phase d'enregistrement une phase « *très critique* » qui « *doit être protégée en conséquence* » : elle recommande de « favoriser une rencontre en présence lors de l'enregistrement d'un facteur inhérent » pour vérifier l'identité et limiter les risques liés au morphing ou spoofing, soulignés par plusieurs interlocuteurs.

⁶⁶ Auxquels s'ajoutent environ 400 dispositifs de recueil en postes consulaires. Source : ANTS

⁶⁷ Les calculs et hypothèses retenus sont présentés et détaillés dans l'annexe consacrée aux différents scénarios, notamment un temps d'enrôlement en face-à-face de 20 minutes.

Rapport

3.3.2. L'enrôlement de l'ensemble des assurés dans un système biométrique par empreintes digitales sur 5 ans coûterait de l'ordre de 1,2 Md€ au moins

Dans ce scénario, l'empreinte ou son gabarit sont stockés dans la carte Vitale, qui intègre un capteur biométrique (cf. graphique 4).

Graphique 4 : Exemple de carte à puce biométrique dotée d'un lecteur d'empreinte digitale



Source : Mission d'après Internet.

À l'usage, lorsque la carte est introduite dans le lecteur, l'algorithme de comparaison vérifie la concordance entre l'empreinte déposée sur le capteur et l'empreinte référencée dans la puce.

Une telle solution nécessite toutefois le remplacement d'une partie du parc actuel de lecteurs de cartes Vitale des professionnels et établissements de santé, sans qu'il soit possible de déterminer leur nombre à ce stade. En effet, l'apposition de l'empreinte sur le lecteur présent sur la carte nécessite que cette dernière soit partiellement découverte. Or, certaines configurations de lecteurs ne remplissent pas ces conditions.

Les limitations précisées *supra* sont ici applicables, en particulier il est à noter que certaines personnes ne seront pas reconnues car les conditions de recueil (température, humidité, etc.) ne permettront pas, en tout cas dans un délai utile, la reconnaissance de leurs empreintes.

La diffusion d'une telle carte risque de mettre en évidence un nombre important d'échecs à l'usage, notamment des faux négatifs empêchant donc des titulaires de droits ouverts de les exercer.

Le taux de rejet d'utilisateurs légitimes qu'on ne pourra pas enrôler est estimé au minimum à 0,096%, soit potentiellement environ 56 000 titulaires de cartes Vitale⁶⁸. Pour les assurés qui auront pu être enrôlés, le GIE SESAM Vitale estime le taux d'échec en conditions d'usage entre 2 % et 5 %, soit entre 1 158 000 et 2 895 000 assurés⁶⁹.

La durée de vie d'une telle carte a été évaluée à environ 5 années au maximum par les industriels, notamment du fait du caractère moins durable de ses composants. Dans l'hypothèse d'un renouvellement tous les cinq ans, près de 12 millions de cartes devraient donc être fabriquées chaque année (sans prendre en compte les cas d'usure anticipée, de perte ou de vol de carte), pour un coût annuel estimé à environ 250 M€ (cf. graphique 5).

⁶⁸ Estimation à partir du parc de cartes Vitale actuel : 57,9 M de cartes.

⁶⁹ Pour les cartes bancaires biométriques qui sont en circulation sur le marché français, il n'a pas été communiqué à la mission par les industriels le taux de rejet en conditions d'utilisation réelles, ni de retour d'expérience des usagers, ce qui tend à accréditer le caractère encore novateur de la solution (quelques dizaines de cartes produites par jour).

Graphique 5 : Scénario d'une carte Vitale biométrique avec capteur d'empreinte digitale (renouvellement du parc sur 5 années)



Source : Mission.

Pour ce chiffrage, des hypothèses structurantes ont été établies, notamment un comportement des assurés inchangés, c'est-à-dire en ne tenant pas compte des effets du prochain déploiement de l'ApCV et de l'effet potentiellement dissuasif de la mise en place d'un contrôle biométrique sur la carte physique, et un coût de fabrication unitaire de la carte de 10 €.

Le coût total d'une telle solution serait ainsi de l'ordre de 1,2 Md€ au moins, à étaler sur 5 ans, hors coût de développement logiciels et matériels, et hors coût de maintien en conditions de fonctionnement du système actuel pendant 5 années.

Ce chiffrage, comme celui *infra* pour la reconnaissance faciale, n'intègre pas le surcoût attendu de la hausse des FSE non sécurisées, du fait d'un déport des assurés vers des justifications non biométriques de leurs droits. La CNAM estime cette hausse de l'ordre de + 5%, entraînant des coûts de gestion supplémentaire de 129 M€ par an.

3.3.1. Le déploiement d'un système biométrique par reconnaissance faciale sur 10 ans s'établirait au moins à 965 M€

Dans ce scénario, une photographie de haute résolution ou un gabarit des traits du visage sont stockés dans la puce de la carte. Afin d'assurer la comparaison avec le visage du porteur de la carte, une caméra frontale est installée sur l'ensemble des postes des professionnels et établissements de santé (service des admissions), soit a minima 410 000 caméras chez les professionnels de santé hors officines, 50 000 en officine, sans compter celles déployées en établissement de santé, de l'ordre de quelques dizaines de milliers.

Ce scénario serait un peu moins onéreux mais n'offrirait pas de meilleures performances que le scénario précédent :

- ♦ à l'enrôlement, le taux de rejet d'utilisateurs légitimes est estimé *a minima* à 1 % par le GIE SESAM Vitale⁷⁰, mais pourrait être moindre du fait de la sécurisation de l'enrôlement en « face-à-face » ;

⁷⁰ Pour l'application carte Vitale et un enrôlement à distance.

Rapport

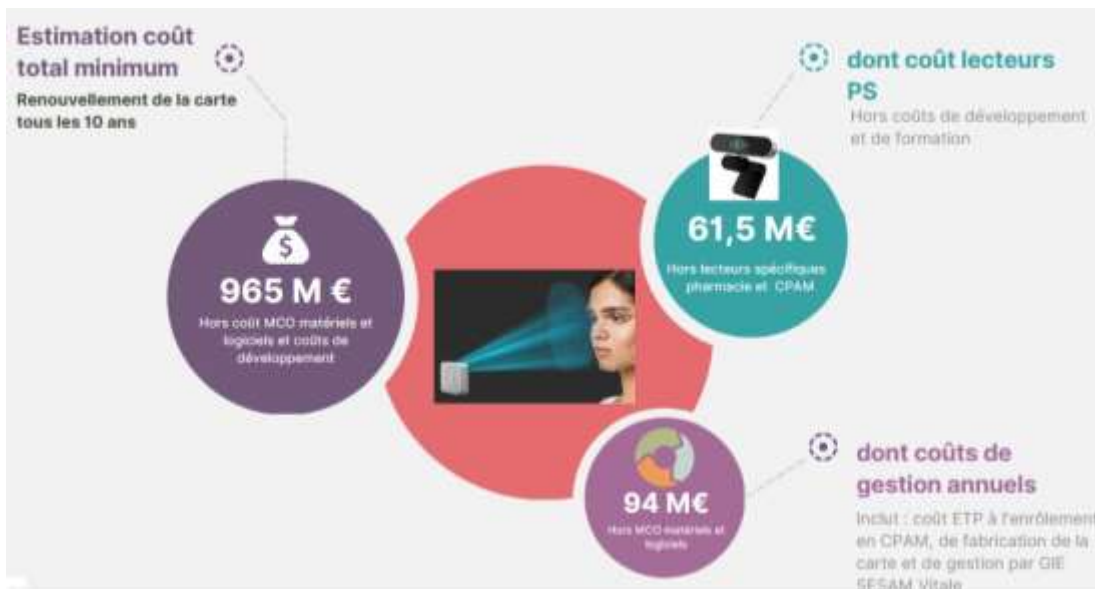
- ◆ à l'usage, le taux d'erreur semble en pratique plus élevé que celui enregistré pour les empreintes digitales (> 5%) en raison notamment de la plus grande sensibilité aux effets du vieillissement, aux conditions de luminosité ou de contraste, au port d'accessoires sur le visage, au positionnement du visage face à la caméra.

Par ailleurs, comme indiqué *supra*, il existe un risque d'erreur à l'usage lié aux biais des algorithmes mis en œuvre.

Finalement, la mise en œuvre d'une telle solution risque de mettre en évidence un nombre important d'échecs à l'usage, probablement supérieurs à ceux estimés pour l'empreinte digitale.

La durée de mise en circulation d'une telle carte a été évaluée à environ 10 années au maximum pour pouvoir renouveler le gabarit biométrique à cette échéance⁷¹. Dans cette hypothèse, 5 790 000 cartes devraient donc être fabriquées chaque année (sans prendre en compte les cas d'usure anticipée, de perte ou de vol de carte), pour un coût annuel estimé à 94 M€ (cf. graphique 6).

Graphique 6 : Scénario reconnaissance faciale (renouvellement du parc sur 10 années)



Source : Mission.

Dans ce scénario, le coût de fabrication unitaire de la carte – qui ne comprend pas de lecteur d'empreinte digitale – est de 5 €. L'hypothèse d'un comportement des assurés inchangé est conservée.

Le coût total d'une telle solution s'établirait ainsi au moins à 965 M€ sur 10 ans, hors coût de développement logiciels et matériels et hors coût de maintien en conditions de fonctionnement du système actuel pendant 10 années.

3.3.2. Certains coûts et risques supplémentaires doivent également être pris en compte

Des surcoûts seraient par ailleurs induits du fait des contraintes opérationnelles qu'il est difficile de chiffrer à ce stade, découlant :

⁷¹ Sauf à accepter une dégradation sensible du taux de rejet.

Rapport

- ◆ des mesures de sécurité du dispositif (cf. règlement de l'UE eIDAS), qui devront donner des garanties suffisantes pour maîtriser le risque de compromission des données ;
- ◆ du nécessaire développement d'un système d'information et de gestion des centaines de milliers d'anomalies (traitement des faux négatifs) ;
- ◆ de la majoration du nombre de FSE dégradées ou papier en résultant ;
- ◆ de l'augmentation du coût de production en termes de développement durable⁷².

Enfin, s'agissant d'une carte contenant des données personnelles irrévocables et conditionnant le bon fonctionnement du système de facturation des soins d'une population entière, il convient d'attirer l'attention sur l'accroissement de l'exposition de l'assurance maladie (et de la nation) aux risques suivants :

- ◆ la production d'un plus grand nombre de cartes accroît la dépendance technologique aux industriels, fournisseurs de normes et composants, dont une partie sont fabriqués à l'étranger (exposition au risque de pénurie) ;
- ◆ le risque réputationnel en cas d'obsolescence technologique du composant sécuritaire de la puce et de piratage de la donnée biométrique ;
- ◆ une dépendance technologique avec l'industriel retenu, dans l'hypothèse d'un stockage sur la puce de la donnée sous la forme d'un gabarit propriétaire.

3.4. L'usage de la biométrie fait l'objet des plus vives réticences de la part des professionnels de santé, qu'ils exercent en ville ou en établissement

La mission a conduit des auditions larges pour recueillir les avis de la communauté soignante sur un éventuel projet de mise en place d'une carte Vitale biométrique. L'usage de la biométrie fait l'objet d'un ample rejet de la part des interlocuteurs, aussi bien en ville qu'en établissement de santé.

3.4.1. Les professionnels de santé libéraux critiquent l'inutilité de la mesure et insistent sur les risques associés

Les professionnels de santé libéraux, qu'ils expriment une position syndicale, ordinale ou personnelle, insistent sur les inconvénients associés à l'usage de la biométrie : perte de temps médical ou paramédical du fait de l'ajout d'un contrôle administratif (et, le cas échéant, du traitement dérogatoire des rejets), caractère intrusif de la mesure alors que c'est une relation de confiance qui fonde les échanges entre patient et soignant, inutilité de cet usage pour la fraction, souvent importante, de patientèle déjà connue par le professionnel. Le caractère incongru d'un tel contrôle a été souligné lorsque le professionnel de santé se déplace au domicile du patient.

Le contrôle biométrique suscite également des craintes :

- ◆ avant tout, du risque d'incivilité en cas de rejet du traitement d'authentification ;
- ◆ de difficultés prévisibles dans les pharmacies d'officine où une partie importante (entre un tiers et la moitié d'après les interlocuteurs) de la patientèle vient aujourd'hui chercher des médicaments pour le compte d'un tiers⁷³ avec prêt légitime de la carte Vitale.

⁷² À ce stade les industriels ne se prononcent pas sur la possibilité de produire de telles cartes à partir de matériaux recyclés.

⁷³ Souvent un membre de la famille, une assistante maternelle, une aide à domicile présente une ordonnance pour le compte d'une personne malade ou étant dans l'incapacité de se déplacer, d'un enfant mineur, du conjoint, d'une personne âgée ou handicapée, résidente en EHPAD, personne sous tutelle ou curatelle.

Rapport

Surtout, les professionnels de santé craignent d'être mis en difficulté en cas de détection d'une fraude à l'identité :

- ◆ ils ne peuvent en pratique refuser les soins, engageant leur responsabilité disciplinaire ;
- ◆ ils ne peuvent non plus facturer ceux-ci à l'assurance maladie, engageant également en ce cas leur responsabilité disciplinaire dans le cadre ordinal (participation à une fraude).

Par ailleurs, l'hypothèse d'investissements supplémentaires dans des logiciels et des matériels, et notamment dans des lecteurs biométriques, les conduiraient à solliciter des aides financières des pouvoirs publics.

A contrario, ils accueilleraient plus favorablement un dispositif s'intégrant aux projets en cours de déploiement de l'INS et de l'application carte Vitale et qui aille dans le sens de la simplification du parcours des patients et de leur équipement de cabinet (logiciel et matériel) tout en maintenant la garantie de paiement.

3.4.2. Pour les professionnels exerçant en établissement, l'usurpation d'identité est un problème de santé publique limité qui n'empêche pas la délivrance du soin

L'organisation spécifique des établissements de santé, avec souvent une structure administrative en charge des admissions et de la facturation distincte de la structure assurant les soins, conduit à une problématique différente.

Du point de vue des services soignants, le sujet de la fraude à l'identité est d'abord perçu comme une difficulté en termes d'identitovigilance, et donc de qualité et de sécurité des soins. Les soignants rencontrés ont unanimement relevé leur obligation déontologique de soigner les patients, indépendamment de la prise en charge ou non par l'assurance maladie (ou par l'État si des droits à l'AME étaient ouverts).

Ainsi, la détection d'une usurpation d'identité n'emporte comme conséquence qu'un échange avec l'usurpateur sur les conséquences sanitaires néfastes de celle-ci (compromission du dossier médical) sans remettre en cause les soins à prodiguer.

Du point de vue des services administratifs chargés de la facturation, l'ajout d'un contrôle biométrique viendrait alourdir la procédure d'admission, dès lors que la carte Vitale n'est guère plus utilisée par les établissements que pour en extraire le NIR du patient, les droits étant consultés via le téléservice CDRi (cf. supra). Au demeurant, une partie non négligeable des admissions est réalisée par un tiers pour le compte du patient.

Surtout, l'usage de la biométrie viendrait à contre-courant du mouvement de dématérialisation de la préadmission à distance engagé par les établissements, qui investissent fortement dans ces solutions afin de réduire les coûts mais aussi fluidifier les parcours patients. Les établissements de santé se trouveraient confrontés à une forme d'injonction paradoxale : dématérialiser et fluidifier le parcours pour plus de confort pour le patient et d'efficacité pour l'établissement, tout en bloquant et contrôlant physiquement l'assuré afin de lutter contre la fraude à l'usurpation d'identité.

3.5. La CNIL n'est pas favorable aux scénarios biométriques présentés

Saisie par la mission, la CNIL⁷⁴ a indiqué qu'elle n'était pas favorable à la mise en œuvre des scénarios biométriques présentés ci-dessus : « compte tenu à la fois de la sensibilité des données en cause, des conséquences prévisibles pour la prise en charge sanitaire des personnes et des potentiels détournements d'usage de ces traitements, [ils] présentent le niveau de risques le plus élevé d'atteintes à la vie privée et aux libertés individuelles ».

S'agissant de l'architecture retenue, elle écarte en outre le recours à une base centralisée, « le recours à des dispositifs d'authentification biométriques pour s'assurer de l'identité d'une personne peut être considéré comme acceptable dès lors que les données biométriques sont conservées dans un support individuel et non dans une base centralisée ».

4. Une solution alternative à la biométrie est envisageable : la CNiE et les titres de séjour pourraient porter le NIR de l'assuré

L'inscription du NIR sur les titres d'identité régaliens représente une solution alternative qui cumule les avantages en termes de lutte contre la fraude, d'identitovigilance, de simplicité d'utilisation et d'accès aux droits. Le titre d'identité sécurisé porteur du NIR aurait vocation à se substituer à la carte Vitale physique.

Ce dispositif offrirait une articulation judicieuse avec l'application carte Vitale une fois que celle-ci sera généralisée. Dans ce scénario, l'assuré aurait donc à terme un moyen dématérialisé sécurisé pour attester de ses droits, l'application carte Vitale, un support physique sécurisé, le titre d'identité sécurisé porteur du NIR, un support physique simple, l'attestation de droits en format papier.

4.1. Cette solution, cohérente avec la stratégie développée par les pouvoirs publics en matière de santé et d'e-santé poursuit plusieurs finalités d'intérêt général

L'inscription du NIR sur les titres d'identité régaliens - carte nationale d'identité électronique (CNiE) ou titre de séjour (TS) – constitue un scénario alternatif à la carte Vitale biométrique en matière de lutte contre la fraude comme s'agissant de l'identitovigilance. Il permettrait, en outre, de fiabiliser la facturation.

Un tel scénario présente plusieurs avantages :

- ◆ **il répond à l'enjeu de lutte contre la fraude à l'usurpation d'identité**, tout en simplifiant les démarches administratives des usagers :
 - la photographie sur la carte nationale d'identité est récente et de bonne qualité ;
 - la procédure de délivrance et de renouvellement est sécurisée en face-à-face ;
 - le prêt, par exemple pour aller chercher un médicament à la pharmacie, sera toujours possible, mais les usagers prêtent leur CNiE ou leur TS *a priori* moins facilement que leur carte Vitale ;
 - enfin apposer le NIR dans la CNiE ou le TS revient à supprimer une formalité administrative, la demande d'une carte Vitale, pour les usagers.

⁷⁴ Courrier MLD/AGN/CR231149 de la Présidente de la CNIL à la mission IGAS-IGF, en date du 13 mars 2023 ; saisine n° 23001970.

Rapport

- ◆ un tel projet contribuerait à un objectif de santé publique en s'inscrivant en **cohérence** avec la généralisation de l'INS dans un objectif de **sécurité sanitaire (identitovigilance) et de protection de la santé publique**. La banalisation de la présentation du titre d'identité porteur du NIR par l'utilisateur permettrait aux professionnels de santé de répondre aux exigences qui s'imposent en matière d'identitovigilance, puisqu'il pourrait ainsi qualifier l'INS.
- ◆ **il permettrait d'apporter des réponses à deux lacunes majeures** du processus de facturation, potentiellement coûteuses en termes de gestion ou génératrices de complexité administrative pour les usagers :
 - **les difficultés nées du rattachement des enfants mineurs à la carte Vitale de leurs parents (et des mineurs/majeurs protégés)**, qui pose des difficultés récurrentes de prise en charge (cf. 2.3.3) ;
 - **les rejets de paiement faute de mise à jour en temps réel de la carte Vitale** puisque l'appel systématique à un téléservice, sur la base du NIR contenu dans la CNIe ou le TS, permettrait de consulter les droits en temps réels et ainsi de réduire près de la moitié des rejets de facturation dus à l'absence d'actualisation des droits inscrits en carte Vitale ;

Par ailleurs, la présence d'une puce NFC permettrait de conserver la signature électronique des feuilles de soins et d'accorder une garantie de paiement aux professionnels ou établissements de santé.

Au demeurant, des solutions similaires ont déjà été mise en œuvre et fonctionnent dans plusieurs pays européens⁷⁵ dont les assurés utilisent un document national d'identité pour s'identifier dans leur système de santé (Belgique, Suède, Portugal – cf. encadré 3). Le Danemark envisage également, dans les prochaines années, de remplacer la carte de santé par une nouvelle carte d'identité nationale sécurisée dans une optique de lutte contre la fraude⁷⁶.

Encadré 3 : L'exemple du Portugal

Depuis 2007, le Portugal a mis en place une nouvelle « carte du citoyen », qui remplit la fonction de carte nationale d'identité et contient également le numéro de sécurité sociale et le numéro d'utilisateur de santé : le premier est utilisé pour l'identification et l'accès aux services de sécurité sociale et le second pour l'accès aux services de santé publique (hôpitaux, centres de santé, postes médicaux).

Tous les citoyens, dès leur naissance, disposent d'une carte de citoyen avec leurs numéros d'identification d'utilisateur civil, fiscal, sanitaire et de sécurité sociale. Des certificats électroniques d'authentification et de signature qualifiée (QDS), permettent aux usagers de s'authentifier auprès de services informatisés, à distance ou localement.

Le nombre de cartes physiques en circulation est 11 millions. Le nombre de cartes dématérialisées est de 650 000 (soit un taux de couverture proche de 100 % des ressortissants).

La carte est présentée à chaque rendez-vous, pour l'identification du patient. Elle est sécurisée par un code PIN. Sa durée de validité est de 10 années. Pour les nouveau-nés, elle est gratuite jusqu'à leurs 20 premiers jours. La puce n'est mise à jour que lors du renouvellement du document.

Ce scénario a souvent été proposé spontanément par plusieurs interlocuteurs de la mission et a été généralement bien accueillie par les personnes rencontrées (ordres, professionnels, syndicats, fédérations, établissements).

⁷⁵ Le règlement (UE) 2019/1157 permet aux Etats membres d'intégrer sur la puce d'un titre d'identité ou de séjour d'autres données que celles nécessaires à la preuve de l'identité du titulaire.

⁷⁶ Cf. annexe VIII.

Rapport

4.2. Le déploiement opérationnel sera progressif et articulé avec le calendrier de généralisation de l'application carte Vitale

L'intégration du NIR dans la CNIe ou le TS se ferait par l'ajout dans la puce d'un container spécifique à l'assurance maladie, séparé de façon étanche de l'identité régalienne et lisible uniquement par les professionnels et établissements de santé habilités⁷⁷.

Le NIR pourrait également être intégré au QR code 2D-DOC figurant au verso de la nouvelle carte nationale d'identité (entouré en vert dans la photo ci-dessous), notamment pour faciliter sa lecture par les employeurs ou Pôle emploi⁷⁸.

Graphique 6 : Verso d'une CNIe



Rapport

Enfin, un déploiement pourrait être progressif sur une dizaine d'années, au rythme actuel d'émission de 6 millions de CNIe par an, et intervenir une fois mené à bien le déploiement de l'ApCV et notamment l'équipement des professionnels de santé et la montée en charge de l'infrastructure, puisque la même architecture sera utilisée.

Le directeur général de la CNAM a toutefois fait part de ses « *très fortes réserves* »⁸¹, concernant ce projet. Plusieurs motifs sont soulevés notamment le fait que ce scénario ne répondrait à aucun besoin ou enjeu, en termes de lutte contre la fraude ou en termes de simplification administrative, qu'il pourrait fragiliser le déploiement dans un futur proche de l'ApCV, qu'il ne permettrait pas de couvrir à lui seul l'ensemble de la population assurée et qu'il présenterait plusieurs risques techniques et d'image.

Certaines de ces interrogations doivent faire l'objet de travaux approfondis (cf. *infra*) pour préciser le cadre de fonctionnement précis d'une telle solution et déterminer dans quelle mesure les difficultés techniques et la pleine couverture des assurés pourraient être résolues.

Il semble toutefois à la mission que :

- ◆ le portage du NIR sur les pièces d'identité rendrait les fraudes à l'usurpation d'identité plus difficiles, tout en simplifiant pour les usagers leurs démarches quotidiennes ; pour les professionnels de santé, notamment en ville, il permettrait de qualifier l'INS dans une optique de sécurité sanitaire, tout en donnant accès aux droits à jour de l'assuré ;
- ◆ le développement puis déploiement d'un tel projet ne pourrait intervenir – et n'aurait de sens – qu'après la généralisation réussie de l'application carte Vitale, en séparant bien les deux temporalités ; ce scénario s'inscrirait en pleine complémentarité avec l'ApCV, en offrant la possibilité aux usagers de posséder un support physique alternatif à l'application (lorsque l'utilisateur ne possède pas de smartphone, qu'il n'a pas souhaité installer l'appli, ou que son smartphone est déchargé, voire volé).

4.3. En première approche, les éléments avancés par la CNIL ne sont pas bloquants

Sollicitée par la mission sur ces différents scénarios, la CNIL⁸² considère ce scénario moins intrusif que la biométrie et moins risqué d'un point de vue technique. Elle a indiqué que sa mise en place suppose qu'un motif d'intérêt public important le justifie et soit démontré.

Elle établit, de surcroît, une liste de prérequis impératifs suivants :

- ◆ assurer l'étanchéité du container « assurance maladie » par rapport aux autres données contenues dans la puce du titre ;
- ◆ garantir l'existence de canaux distincts afin que les services municipaux et préfectoraux n'accèdent pas au NIR des personnes établissant leur CNIe ou leur TS ;
- ◆ s'assurer de l'application du secret professionnel aux accédants du NIR aux fins de création et de délivrance des titres d'identité ;
- ◆ prévoir la possibilité de s'opposer à l'inscription du NIR sur son document d'identité⁸³ ;
- ◆ s'assurer de l'existence de voies alternatives pour faire valoir ses droits sociaux.

Si ces éléments appellent une réponse spécifique, aucun ne semble, en première approche, empêchant.

⁸¹ Cf. Annexe IX.

⁸² Courrier MLD/AGN/CR231149 de la Présidente de la CNIL à la mission IGAS-IGF, en date du 13 mars 2023 ; saisine n° 23001970. Cf. Annexe VII.

⁸³ De fait, les personnes nées à l'étranger avant 1970 et n'ayant jamais été affiliées à la sécurité sociale française ont le droit de se voir établir une CNIe, mais ne disposent pas de NIR.

Rapport

À l'instar de la CNIL, la mission considère que ce scénario devrait être approfondi par des travaux menés conjointement par les ministères de l'Intérieur et de la Santé aux fins d'étudier plus précisément les modalités techniques et juridiques nécessaires à sa mise en œuvre.

À Paris, le 26 avril 2023

Les membres de la mission,

L'inspectrice générale
des affaires sociales,

Carole Lépine

L'inspecteur des finances,

Hadrien Haddak

L'inspecteur général
des affaires sociales,

Vincent Ruol

L'inspecteur des finances,

Adrien Bayle

Sous la supervision de
l'inspecteur général
des finances,

François Auvigne

ANNEXES ET PIÈCE JOINTE

LISTE DES ANNEXES ET DE LA PIÈCE JOINTE

ANNEXE I :	LA CARTE VITALE
ANNEXE II :	LES CARTES VITALE SURNUMÉRAIRES ET LES RÉSIDENTS AFFILIÉS À L'ASSURANCE MALADIE
ANNEXE III :	LA LUTTE CONTRE LA FRAUDE AUX PRESTATIONS D'ASSURANCE MALADIE ET LA FRAUDE LIÉE À L'USAGE DES CARTES VITALE
ANNEXE IV :	L'APPLICATION CARTE VITALE
ANNEXE V :	LE RECOURS À LA TECHNOLOGIE BIOMÉTRIQUE : AVANTAGES ET INCONVÉNIENTS
ANNEXE VI :	SCÉNARIOS D'UNE CARTE VITALE BIOMÉTRIQUE
ANNEXE VII :	ANALYSE JURIDIQUE <ul style="list-style-type: none">◆ PJ1 : AVIS DE LA CNIL◆ PJ2 : RÉPONSE DE LA DAJ DES MINISTÈRES SOCIAUX
ANNEXE VIII :	PARANGONNAGE INTERNATIONAL
ANNEXE IX :	CONTRIBUTIONS ÉCRITES <ul style="list-style-type: none">◆ PJ1 : CONTRIBUTION DE LA FÉDÉRATION HOSPITALIÈRE DE FRANCE◆ PJ2 : CONTRIBUTION DE L'ORDRE NATIONAL DES MÉDECINS◆ PJ3 : CONTRIBUTION DU CONSEIL NATIONAL DE L'ORDRE DES PHARMACIENS◆ PJ4 : COURRIEL DU DIRECTEUR GÉNÉRAL DE LA CNAM
ANNEXE X :	LISTE DES PERSONNES RENCONTRÉES
PIÈCE JOINTE	LETTRE DE MISSION

ANNEXE I

La carte Vitale

SOMMAIRE

1. LA CARTE VITALE, SUPPORT PERSONNALISÉ ET SÉCURISÉ DES DROITS SOCIAUX DEPUIS 1998, EST UN FACTEUR D'ACCÉLÉRATION DES FLUX DE FACTURATION DÉMATÉRIALISÉ ET DU DÉPLOIEMENT DU TIERS PAYANT	1
1.1. La carte Vitale permet l'identification de l'assuré et la sécurisation des flux de facturation opérés par l'assurance maladie, tout en constituant un support des droits sociaux.....	1
1.2. Le flux SESAM-Vitale établi au moyen de la carte Vitale de l'assuré a permis l'établissement de plus d'1,7 milliards de feuilles de soins électroniques en 2022, sécurisant près de 75% des transmissions de factures à l'assurance maladie	3
1.2.1. <i>Les flux de facturation sécurisés avec la carte Vitale, dits flux SESAM-Vitale, représentent 72% du total des feuilles de soins électroniques émises par les professionnels de santé et permettent un remboursement en moins de quatre jours en moyenne par l'assurance maladie.....</i>	<i>5</i>
1.2.2. <i>La carte Vitale, support de développement du tiers payant, permet aux professionnels de santé de bénéficier d'une garantie de paiement de l'Assurance maladie.....</i>	<i>8</i>
1.2.3. <i>Une infrastructure composée de 410 000 terminaux de lecture des cartes et de logiciels déployés chez les professionnels de santé est régulée et homologuée par le GIE SESAM-Vitale et la CNDA</i>	<i>9</i>
2. S'APPUYANT SUR DIVERSES ÉVOLUTIONS TECHNOLOGIQUES, LE PARC DE CARTES VITALE FAIT L'OBJET D'UNE GESTION RENFORCÉE DEPUIS 2004 AVEC LA MISE EN PLACE DE LISTES D'OPPOSITION MISES À JOUR QUOTIDIENNEMENT	11
2.1. La modernisation du parc de cartes Vitale a répondu à des enjeux de sécurité et à une volonté d'élargir les informations inscrites sur la carte	11
2.1.1. <i>Les fonctionnalités et les données contenues sur la carte Vitale ont peu évolué depuis sa mise en place, malgré le déploiement à partir 2007 de la carte Vitale 2 dotée d'une photographie de l'assuré.....</i>	<i>11</i>
2.1.2. <i>La sécurisation des données contenues dans la carte a nécessité diverses évolutions techniques depuis 1998.....</i>	<i>13</i>
2.2. Un processus de production des cartes Vitale maîtrisé par le GIE SESAM-Vitale pour un coût de production et de gestion s'élevant à 2,63€ par carte Vitale	15
2.2.1. <i>Le GIE SESAM-Vitale conçoit et produit environ 4 millions de cartes Vitale par an pour le compte de ses membres.</i>	<i>15</i>
2.2.2. <i>Le coût total de production d'une carte Vitale est de 2,63 €.....</i>	<i>17</i>
2.3. Le parc de carte Vitale comptait 57,9 millions de cartes valides au 31 décembre 2021, dont 64% de cartes Vitale 2 porteuses de la photo de l'assuré.....	18
2.4. Une faiblesse structurelle du dispositif est liée à son architecture locale et à l'impossibilité de mettre à jour systématiquement les droits inscrits en carte, emportant un préjudice financier potentiellement important pour l'assurance maladie	18
2.4.1. <i>Depuis 2019, environ 80 % des cartes Vitale font l'objet d'une mise à jour annuelle.....</i>	<i>19</i>

2.5. Un système d'opposition a été mis en place à partir de 2004 afin d'améliorer la gestion du parc de cartes Vitale et de répondre aux besoins des différents acteurs du système de santé.....	20
2.5.1. <i>Le système repose sur la base de gestion technique des cartes (GTC) gérée par le GIE SESAM Vitale qui permet d'établir des listes d'opposition diffusées aux acteurs de santé en fonction de leurs besoins.....</i>	20
2.5.2. <i>Trois listes d'opposition sont constituées pour répondre aux besoins des professionnels de santé et des régimes d'assurance maladie.....</i>	22
3. SI L'USAGE DE LA CARTE VITALE S'EST GÉNÉRALISÉ POUR LES SOINS DE VILLE, LES TÉLÉSERVICES DE CONSULTATION DES DROITS RÉDUISENT SON APPORT ET EXPLIQUENT SA FAIBLE UTILISATION DANS LES ÉTABLISSEMENTS DE SANTÉ.....	24
3.1. En complément de la carte Vitale, le développement du téléservice ADRI permet aux professionnels de santé libéraux de consulter les droits à jour des assurés.....	24
3.1.1. <i>Le téléservice ADRI, actualisé quotidiennement, permet de parer à l'absence de mise à jour automatique des droits inscrits sur la carte Vitale</i>	24
3.1.2. <i>Amelipro offre également aux professionnels de santé un accès sécurisé aux informations relatives à leurs patients, à partir du NIR des assurés</i>	25
3.2. En établissement de santé, la consultation des droits est opérée au moyen des services en ligne de consultation des droits (CDR et CDRi) lors de la phase de pré-admission	26
3.2.1. <i>Dans le cadre de soins urgents en établissement de santé, il est fréquent de ne pas présenter de carte Vitale</i>	28
3.2.2. <i>Lors de l'admission dans le cadre de soins programmés, la carte Vitale n'est employée que pour obtenir le NIR des patients afin de consulter CDR ou CDRi afin de vérifier l'existence et la nature des droits sociaux ouverts.....</i>	28

1. La carte vitale, support personnalisé et sécurisé des droits sociaux depuis 1998, est un facteur d'accélération des flux de facturation dématérialisé et du déploiement du tiers payant

1.1. La carte Vitale permet l'identification de l'assuré et la sécurisation des flux de facturation opérés par l'assurance maladie, tout en constituant un support des droits sociaux

La carte d'Assurance maladie « Vitale » est un **support électronique personnalisé et inter-régimes prévu par l'ordonnance du 24 avril 1996¹**, et diffusé à partir de 1998 auprès des assurés sociaux par le GIE SESAM-Vitale.

Encadré 1 : Le GIE SESAM Vitale

L'article L. 115-5 du code de la sécurité sociale dispose que les « *caisses nationales des régimes de base d'assurance maladie peuvent constituer un groupement d'intérêt économique, afin de lui confier des tâches communes de traitement de l'information, à l'exclusion du service des prestations* ».

En application de ce texte, le GIE SESAM-Vitale a été créé le 3 février 1993 par les régimes obligatoires d'assurance maladie. Ils ont été rejoints par les organismes d'assurance maladie complémentaires² (sous la forme de sociétés d'assurance, de mutuelles³ relevant du code de la mutualité ou d'institutions de prévoyance relevant du code de la sécurité sociale) en 2000.

Le GIE a pour objet⁴ « *la mise en œuvre, la normalisation, la gestion et la promotion des systèmes d'échanges sécurisés, dont les flux de facturation et leurs services associés à l'exclusion du service des prestations, utilisés par les offreurs de soins et/ou les usagers du système de santé* ». Il est chargé de concevoir et de mettre en œuvre les dispositifs d'authentification du patient (Carte vitale et prochainement App Carte vitale), d'assurer le maintien en conditions opérationnelles des services de télétransmission des feuilles de soins électroniques et d'authentification du patient, et enfin, plus généralement d'accompagner les industriels, professionnels de santé et assurés sociaux dans la transformation numérique du système de santé, pour son volet facturation.

Sont membres du GIE :

- la Caisse nationale d'assurance maladie (CNAM) ;
- la Caisse centrale de la mutualité sociale agricole (CCMSA) ;
- l'Union nationale des régimes spéciaux (UNRS) ;
- la Mutualité de la fonction publique (MFP) ;
- la Fédération nationale de la mutualité française (FNMF) ;
- France Assureurs ;
- le Centre technique des institutions de prévoyance (CTIP).

Le GIE est constitué avec une durée limitée : sauf modification conventionnel, il sera dissous le 31 décembre 2041.

¹ Ordonnance n° 96344 du 24 avril 1996 portant mesures relatives à l'organisation de la sécurité sociale.

² Sur la base de l'article R. 161-33-9 du code de la sécurité sociale, de portée générale et ne visant pas spécifiquement le GIE SESAM-Vitale, donnant la possibilité aux régimes d'assurance maladie obligatoire de conclure des conventions avec les organisations professionnelles représentant les organismes d'assurance maladie complémentaire.

³ Il convient à ce titre de distinguer l'activité de certaines mutuelles gérant un régime obligatoire de sécurité sociale (à l'époque, mutuelles étudiantes ou de fonctionnaires notamment) de l'activité de gestion d'un régime d'assurance maladie complémentaire.

⁴ Source : convention constitutive.

Annexe I

Les documents budgétaires du GIE SESAM Vitale font apparaître des dépenses totales s'élevant à 56,7 millions 2022 (en hausse de 10,3 millions d'euros par rapport à l'exercice 2021)⁵. Ces dépenses ont été financées à hauteur de 84,8% par la CNAM. En 2022, elles se sont réparties entre les dépenses de fonctionnement du GIE (22,62 millions d'euros) et les dépenses consacrées à divers programmes (34,03 millions d'euros), dont :

- programme Identité numérique Cartes (CV et carte européenne AM) : 8,876 millions d'euros ;
- programme identité numérique ApCV : 4,4 millions d'euros ;
- programme assistance technique (dont flux Sésame-Vitale) : 11 millions d'euros.

Le déploiement de la carte Vitale a fait suite à une **expérimentation entamée en novembre 1987**, s'appuyant sur une carte à micro-processeur contenant les informations administratives de l'assuré et de ses ayants-droit. Les habitants de quatre communes d'Ille-et-Vilaine⁶, dépendant du régime général d'assurance maladie et du régime agricole, ont été dotés d'une carte dite SESAM. Cette expérimentation a duré 10 ans, jusqu'au **déploiement de la carte Vitale en 1998**.

Le cadre légal de la carte Vitale est défini à l'article L. 161-31 du code de la sécurité sociale. Les dispositions réglementaires applicables ont été modifiées récemment par **le décret n° 2022-1719 du 28 décembre 2022 relatif aux moyens d'identification électronique inter-régimes mentionnés aux articles L. 161-31 et L. 161-33 du code de la sécurité social**, et figurent aux articles R. 161-33-1 à R. 161-33-21 du code de la sécurité sociale. Le dispositif juridique applicable est complété par les arrêtés du 14 mars 2007 relatifs, respectivement « *aux conditions d'émission et de gestion des cartes d'assurance maladie* » et « *aux spécifications physiques et logiques de la carte d'assurance maladie et aux données contenues dans cette carte* ».

L'article L. 161-31 du code de la sécurité sociale ne prévoit **pas d'obligation de détention d'une carte Vitale**, qui demeure une faculté. L'assuré social peut exercer ses droits en produisant une attestation de droits sous forme papier.

La carte Vitale est :

- ◆ un **support de l'identité de l'assuré**, telle qu'elle est connue des régimes d'assurance maladie obligatoire et de celle des ayants-droit⁷ :
 - cette identité est fondée sur le numéro d'inscription au répertoire (NIR), qui reprend en principe les traits d'identité définis à l'état-civil pour les personnes nées en France ;
 - ce numéro d'assuré social, défini dans les jours qui suivent la naissance, se distingue des autres numéros d'identité attribués par l'administration :
 - numéros de carte nationale d'identité ou de passeport pour le ministère de l'intérieur ;
 - numéro fiscal pour le ministère de l'économie et des finances ;
 - numéro de matricule pour le ministère des armées ;
 - numéro d'étudiant (identifiant national élève, INE) pour le ministère de l'enseignement supérieur.
- ◆ un **support des droits ouverts auprès des régimes d'assurance maladie obligatoire** (AMO), facilitant leur exercice dans un environnement dématérialisé et numérique ;

⁵ En 2021, le budget total du GIE SESAM-Vitale s'élevait à 46,3 millions d'euros.

⁶Châteaubourg, Saint-Didier, Domagné et Saint-Jean-sur-Vilaine.

⁷ Personne qui tient son droit à l'assurance maladie-maternité du fait de ses liens avec un assuré de plus de 16 ans. Ce statut prend fin l'année des 18 ans de l'ayant-droit.

Annexe I

- ◆ un **outil de signature électronique qui sécurise les flux électroniques de facturation (feuille de soins électronique ou « FSE »)** et permet le remboursement des frais de santé sous une semaine sans avoir besoin d'envoyer à l'Assurance maladie une feuille de soins papier.

De manière très accessoire, la carte Vitale peut avoir d'autres fonctions :

- ◆ sa simple présentation à un médecin conventionné ou exerçant en établissement ou centre de santé exprime le consentement à la consultation des relevés de remboursements d'assurance maladie du titulaire de la carte Vitale⁸ (voir 2.1.1) ;
- ◆ elle permet de consulter, d'alimenter et de clôturer le dossier médical partagé de son porteur (CSS, art. R. 161-33-7).

Encadré 2 : Carte vitale et justification d'identité

Aux termes de l'article premier de la loi n° 2012-410 du 27 mars 2012 relative à la protection de l'identité, « *l'identité d'une personne se prouve par tout moyen. La présentation d'une carte nationale d'identité ou d'un passeport français en cours de validité suffit à en justifier* ».

La carte Vitale n'est pas un document d'une valeur probante suffisante pour prouver son identité, même si elle peut y concourir (l'identité se prouvant par tout moyen, donc y compris au moyen d'une carte Vitale, comme par exemple d'une licence de club sportif ou d'une carte d'accès à une bibliothèque).

En matière électorale, la carte Vitale, lorsqu'elle est munie d'une photographie, permet de justifier son identité au sens de l'article R. 40 du code électoral (article premier – citoyens français – et 2 – citoyens européens – de l'arrêté du 16 novembre 2018 (JORF du 21 novembre 2018) modifié) qui régit les opérations de vote. Toutefois, elle ne permet pas de justifier de son identité dans les opérations d'inscription sur les listes électorales.

1.2. Le flux SESAM-Vitale établi au moyen de la carte Vitale de l'assuré a permis l'établissement de plus d'1,7 milliards de feuilles de soins électroniques en 2022, sécurisant près de 75% des transmissions de factures à l'assurance maladie

La carte Vitale est un élément central de la politique de développement de la feuille de soins électronique (FSE) conduite depuis 1998 par l'assurance maladie, qui incite les professionnels de santé à recourir à la télétransmission au moyen d'incitations financières et d'accompagnement technique.

La télétransmission des FSE repose sur un **système d'échanges de données informatisé entre les différents organismes** lors d'un acte de soin :

- ◆ échange entre le praticien et l'assurance maladie pour la part obligatoire ;
- ◆ échange entre l'assurance maladie obligatoire et le régime complémentaire pour la part complémentaire.

Pour télétransmettre des FSE, le professionnel de santé doit être muni d'une carte de professionnel de santé (CPS) et d'un équipement informatique. Les flux de télétransmissions sont qualifiés selon leurs modalités de sécurisation (SESAM Vitale, SESAM sans Vitale, dégradé, cf. *infra*).

En 2022, **394 148 professionnels de santé, soit 73,5%, étaient équipés pour procéder à la facturation SESAM-Vitale, sur un total de 535 936 professionnels**. 1,7 milliards de feuilles de soins électroniques ont été établies.

⁸ CSS, art. R. 161-31.

Annexe I

La carte CPS est délivrée aux professionnels de santé. Valable trois ans, elle est renouvelée automatiquement. Elle est gratuite pour le professionnel de santé.

Le système de facturation SESAM-Vitale est accessible soit par un logiciel installé sur l'ordinateur du professionnel de santé, soit via un navigateur internet, directement en ligne. Il existe également des solutions autonomes reposant sur un lecteur de cartes Vitale et CPS, et intégrant un logiciel de facturation SESAM-Vitale. **L'agrément des logiciels de facturation** est assurée par un service dédié de l'assurance maladie, le Centre National de Dépôt et d'Agrément (CNDA).

L'émission de feuilles de soins électroniques (FSE) présente un triple avantage :

- ◆ **pour l'Assurance maladie, la chaîne de liquidation et de facturation est dématérialisée de manière native**, sans nécessité de recourir à du personnel pour traiter les feuilles de soins papier, avec les risques d'erreur et les délais inhérents :
 - d'après le GIE SESAM-Vitale, le coût de traitement d'une FSE s'établirait à 0,27 € contre 1,74 € pour une feuille de soins papier ;
 - la mise en place de la feuille de soins électronique (FSE) a ainsi permis d'effectuer des gains de productivité importants. **Pendant la période 2014-2017, des gains de productivité de l'ordre de 1 000 ETP⁹ auraient été ainsi obtenus ;**
- ◆ **pour les patients** et de manière corrélative, le processus est accéléré, ce qui permet des **remboursements en une semaine** environ, tout en réduisant les démarches engendrées par la feuille de soins papier ;
- ◆ **pour le professionnel de santé**, les feuilles de soins électroniques établies à partir des informations inscrites dans la carte Vitale (qu'elle soit ou non à jour) lui garantissent, pour les actes pour lesquels l'assuré social bénéficie de l'avance de frais, un **paiement garanti sous sept jours ouvrés¹⁰**, et **facilitent le suivi de la facturation**.

Encadré 3 : Les feuilles de soins électroniques SESAM-Vitale

Les feuilles de soins électroniques (FSE) permettent aux professionnels de santé de facturer les actes aux régimes d'assurance maladie dont dépendent les patients qu'ils prennent en charge.

Schématiquement, une FSE comprend :

- les caractéristiques des actes réalisés (données de santé) ;
- les éléments identifiant le professionnel de santé ;
- les éléments identifiant le patient.

L'identification du professionnel de santé se fait au moyen de la carte de professionnel de santé (CPS). Le patient est, lui, identifié grâce à sa carte Vitale.

En principe, la FSE sécurisée (flux SESAM-Vitale) ne peut être émise que si les cartes CPS et Vitale sont simultanément présentes sur le poste de travail du professionnel de santé. En pratique, les logiciels des professionnels de santé conservent la trace des cartes Vitale qui ont été passées de sorte qu'il est possible pour un professionnel de santé d'émettre des FSE sécurisées, même en l'absence de carte Vitale (par exemple en cas d'oubli).

Il existe toutefois des flux, dits « SESAM sans Vitale », ne nécessitant pas la présence de la carte Vitale lors de leur émission. Il s'agit des actes de biologie (car le professionnel de santé travaille une fois le prélèvement à analyser effectué, et donc le plus souvent en l'absence du patient) et des actes relatifs à la santé sexuelle des mineurs (afin que les flux demeurent anonymes, en particulier envers les parents de la personne mineure concernée), ainsi que la location de matériel médical.

⁹ Cf. Évaluation de la convention d'objectif et de gestion 2014-2017 de la CNAMTS - qualité de service et organisation du réseau, rapport IGAS [2017-008R], septembre 2017.

¹⁰ Et le versement de pénalités aux praticiens en cas de retard de paiement par l'assurance maladie.

1.2.1. Les flux de facturation sécurisés avec la carte Vitale, dits flux SESAM-Vitale, représentent 72% du total des feuilles de soins électroniques émises par les professionnels de santé et permettent un remboursement en moins de quatre jours en moyenne par l'assurance maladie

1.2.1.1. Il existe trois types de flux pour la transmission des feuilles de soins électroniques, selon leur degré de sécurisation

Historiquement, les feuilles de soins étaient complétées par les professionnels de santé et transmises sous format papier au régime d'assurance maladie de l'assuré.

À partir de 1998, le déploiement des cartes Vitale a permis de développer l'établissement de feuilles de soins électronique (FSE) et leur transmission dématérialisée et asynchrone¹¹ aux régimes d'assurance maladie (obligatoire et complémentaire).

Dans le système actuel, **les professionnels de santé peuvent** au moyen de leur carte de professionnel de santé (CPS), **émettre trois catégories de flux FSE** :

- ◆ **flux « SESAM Vitale » sécurisé** (72% des FSE transmises en 2022¹²) :
 - le mode de transmission sécurisé est possible lorsque la **signature est effectuée conjointement par la carte Vitale du patient et la CPS** ;
 - il permet d'authentifier l'acte et de recueillir la signature du patient (voir *supra*), matérialisé par la présence de sa carte Vitale ;
 - la **garantie de paiement**¹³ s'applique à ce flux ;
- ◆ **flux « SESAM sans Vitale » sécurisé** (13% des FSE en 2022) : pour certains actes médicaux spécifiques (biologie, santé sexuelle des mineurs, téléconsultation), ou pour la location de dispositifs médicaux ;
 - malgré l'absence de la carte Vitale du patient, ces flux sont considérés comme sécurisés et traités par les chaînes de facturation de l'assurance maladie comme des flux SESAM-Vitale sécurisés, la **garantie de paiement** s'applique à ces flux ;
 - il s'agit d'un **tenir compte de la nature des soins** (pour les téléconsultations¹⁴, le professionnel de santé n'est pas en présence du patient et de sa carte Vitale ; l'anonymat est souhaité pour la délivrance d'un contraceptif d'urgence à une mineure) ;
- ◆ **flux SESAM Vitale dégradé, dit flux B2** (15% des FSE en 2022) :
 - ce mode de transmission est une alternative au mode sécurisé ;
 - il permet de créer une FSE en présence **uniquement de la carte CPS et sans la carte Vitale du patient**¹⁵.
 - outre la FSE en mode dégradé, le **professionnel de santé doit également transmettre une feuille de soins papier revêtue de la signature du patient**, afin d'attester de sa présence (cf. encadré 4).

¹¹ Les flux ne sont pas nécessairement envoyés au moment de la réalisation de l'acte mais peuvent l'être le soir, voire plusieurs jours après.

¹² Période de 12 mois allant de décembre 2021 (inclus) à novembre 2022 (inclus), données GIE-SESAM-Vitale.

¹³ Cf. 1.2.2

¹⁴ Avenant n° 18 « télémédecine » au cahier des charges SESAM Vitale.

¹⁵ Ce mode peut également être mobilisé pour passer à nouveau un flux SESAM-Vitale sécurisé qui aurait été rejeté : le patient n'étant plus présent, il ne peut signer la nouvelle FSE au moyen de sa carte Vitale.

Annexe I

Le GIE SESAM-Vitale assure un suivi des télétransmissions de FSE et regroupe les deux premiers flux (SESAM-Vitale sécurisé et SESAM sans Vitale sécurisé), au sein des flux « certifiés », par opposition aux flux dégradés. Entre 2015 et 2021, la part des FSE certifiées transmises par les professionnels de santé est restée relativement stable, à des taux compris entre 86% et 92% du total des FSE transmises (cf. tableau 1).

Tableau 1 : Évolution de la part des feuilles de soins électroniques (FSE) certifiées dans les flux de FSE entre 2015 et 2021

Données	2015	2016	2017	2018	2019	2020	2021
Total de feuilles de soins électroniques(FSE), en millions	1 417	1 393	1 371	1 361	1 315	1 403	1 624
Évolution annuelle (en %)	NC	-2%	-2%	-1%	-3%	6,7%	15,8%
Part des FSE certifiées dans le total FSE (en %)	88,8%	89,6%	90,3%	91,2%	91,8%	86,1%	85,7%
Part des FSE dégradées dans le total FSE (en %)	11,2%	10,4%	9,7%	8,8%	8,2%	13,9%	14,3%

Source : GIE SESAM-Vitale

1.2.1.2. Le déploiement des FSE s'est accompagné d'incitations financières pour les professionnels de santé

Afin de sécuriser les flux de facturation, le déploiement des FSE s'est accompagné d'incitations financières liées à l'utilisation de la carte Vitale.

Le taux de télétransmission est ainsi l'un des indicateurs mesurés pour la rémunération de certains professionnels de santé :

- ◆ forfait structure pour les médecins¹⁶ ;
- ◆ rémunération sur objectif de santé publique (ROSP) pour les pharmaciens¹⁷ ;
- ◆ forfait d'aide à la modernisation et informatisation du cabinet professionnel pour les infirmiers¹⁸.

Les feuilles de soins électroniques font également l'objet d'une **rémunération conventionnelle**. À titre d'illustration, pour les pharmaciens : la télétransmission des feuilles de soins électroniques (FSE) en mode SESAM-Vitale permet de bénéficier d'une aide financière à la télétransmission, prévue par la convention nationale des pharmaciens titulaires d'officine¹⁹ et par la convention nationale des pharmaciens mutualistes²⁰ Elle est versée par l'Assurance Maladie. Le versement a lieu au mois de mars de chaque année, au titre des FSE réalisées l'année précédente.

¹⁶ Pour son volet 1, le forfait structure prévoit un objectif (parmi six indicateurs) de FSE supérieur à 2/3, pour une rémunération totale pouvant aller jusqu'à 2 800 €.

¹⁷ À compter de 2022, les pharmaciens perçoivent 0,064€ par FSE lorsque leur taux de télétransmission est inférieur à 95% et 0,07€ au-delà de 95%.

¹⁸ S'ils remplissent les conditions relatives à six indicateurs (dont l'un est un taux de transmission de FSE supérieur à 70%), les infirmiers libéraux se voient accorder un forfait annuel de 490 €.

¹⁹ Journal officiel du 25 juillet 2006.

²⁰ Journal officiel du 14 août 1999.

En 2019, le taux de dématérialisation, tous professionnels de santé confondus, des feuilles de soins atteignait 95,4 %²¹. Les feuilles de soins papier ne représentent ainsi qu'entre 5% et 2% des flux traités par les organismes d'assurance maladie²².

1.2.1.3. Les pharmacies ont recours presque systématiquement à la télétransmission des FSE tandis que d'autres professions de santé sont moins avancées sans qu'il existe de marges de développement significatives

En novembre 2022, d'après les données transmises par le GIE SESAM-Vitale, **73,5% des professionnels de santé ont eu recours à des télétransmissions** de feuilles de soins électroniques (FSE) via les flux SESAM Vitale (soit 394 148 sur une population de référence de 535 936 professionnels de santé).

Les pharmacies, qui représentaient 45% des flux de FSE émis en 2022, ont un taux d'équipement et de recours à la télétransmission de 98,7%. (cf. tableau 2). En conséquence, en dehors de cas spécifiques (médecins spécialistes, opticiens, audioprothésistes, proches de 55%), les taux de recours à la télétransmission par les professionnels de santé peuvent difficilement être augmentés de manière significative et représentent entre les trois quarts et la quasi-intégralité des transmissions de feuilles de soins pour chaque profession de santé considérée individuellement.

Tableau 2 : Taux de recours à la télétransmission par catégories de professionnels de santé :

Professions	Part des professionnels de santé en télétransmission :
Pharmacies	98,7%
Laboratoires	90,5%
Infirmiers	86,2%
Dentistes	84,5%
Médecins généralistes	79,7%
Centres de santé	76,8%
Masseurs-kinésithérapeutes	74,3%
Médecins spécialistes	56,8%
Audioprothésistes	55,8%
Opticiens	54,7%

Source : données en date de novembre 2022, GIE SESAM-Vitale

Encadré 4 : Les feuilles de soins papier accompagnant les flux dégradés

La télétransmission d'un flux dégradé doit s'accompagner de la transmission d'une feuille de soins papier comprenant la signature du patient.

Cette mesure est mal comprise des professionnels de santé, dont beaucoup ont indiqué à la mission signer pour le compte du patient (les feuilles de soins papier comprennent une case « impossibilité de signer » que certains logiciels de cabinet proposent de cocher automatiquement).

Par ailleurs, l'assurance maladie ne dispose pas du spécimen de la signature des assurés sociaux : elle n'est donc pas en mesure de s'assurer de l'authenticité de la signature par le patient de la feuille de soins, qui est précisément la raison pour laquelle elle est exigée.

Cette obligation de signature est donc en l'état inutile en obligeant à un travail administratif supplémentaire le professionnel de santé qui émet des flux dégradés.

²¹ Chiffres clés de la sécurité sociale en 2020, publication de 2021, DSS.

²² Chiffres CPAM du Maine et Loire 2021: FSE : 11 814 186 soit 95,9%, feuilles de soins papier : 505 458 soit 4,1% ; Ain : 2,3% de feuilles de soins papier 13 742 455 feuilles de soins électroniques et 312 135 feuilles de soins papier

Ce dispositif ne présente aucune garantie en matière de lutte contre la fraude.

1.2.2. La carte Vitale, support de développement du tiers payant, permet aux professionnels de santé de bénéficier d'une garantie de paiement de l'Assurance maladie

Pour l'assuré, la carte Vitale permet, le cas échéant, de **bénéficier du tiers payant** et de l'exonération du ticket modérateur. En effet, depuis le 1er janvier 2017, le tiers payant est devenu un droit lorsqu'il s'agit de soins pris en charge à l'occasion d'une maternité et de soins exonérés du ticket modérateur dans le cadre d'une affection de longue durée²³ (ALD). **Pour bénéficiaire de ce droit au tiers-payant, le patient doit présenter sa carte Vitale²⁴.**

Encadré 5 : Le tiers payant

La procédure de tiers payant, dont la généralisation avait été évaluée par l'IGAS en 2017, est applicable de droit dans les cas suivants :

- soins en rapport avec un accident de travail ou une maladie professionnelle ;
- consultations au cours desquelles est prescrit un contraceptif ou des examens de biologie médicale à une mineure d'au moins 15 ans ;
- actes de prévention réalisés dans le cadre d'un dépistage organisé (par exemple, la mammographie effectuée lors du dépistage organisé du cancer du sein) ;
- examens de prévention bucco-dentaire dispensés aux enfants ou adolescents âgés de 6, 9, 12, 15 et 18 ans, ainsi que les soins consécutifs à cet examen, pour les enfants de 6 et 12 ans ;
- actes de lecture différée d'une rétinographie en couleur, sans la présence du patient, par le médecin lecteur dans le cadre du dépistage de la rétinopathie diabétique ;
- honoraires perçus pendant une hospitalisation dans un établissement sous convention avec l'Assurance Maladie, pour la part obligatoire et, le cas échéant, pour la part complémentaire ;
- soins dispensés à un patient bénéficiaire de la Complémentaire santé solidaire (C2S) ;
- soins dispensés à un patient en affection de longue durée (ALD) ou à un patient pris en charge au titre de l'assurance maternité, depuis le 1er janvier 2017 ;
- soins dispensés à un patient bénéficiaire de l'aide médicale d'État (AME) ;
- soins dispensés dans le cadre de la permanence des soins (intervention suite à régulation ou du centre d'appel de l'association de permanence des soins), pour la part obligatoire ;
- examens et soins dispensés à une patiente enceinte exposée au virus Zika ;
- soins en lien avec un acte de terrorisme.

Enfin, depuis le 1er janvier 2017, le tiers payant sur la part obligatoire peut également être proposé à tous les patients.

Pour les professionnels de santé, l'usage de la carte Vitale permet l'application de la garantie de paiement lors de l'établissement d'une feuille de soins électronique (FSE) sécurisée avec la carte Vitale du patient et sans forçage²⁵.

²³ Code de la sécurité sociale, [article L162-1-21](#)

²⁴ Code de la sécurité sociale, article L. 161-36-4.

²⁵ Action du professionnel permettant d'établir une FSE et un flux de facturation sécurisé, en l'absence de carte Vitale.

Annexe I

Dans les cas où les **droits inscrits sur la carte Vitale ne sont pas à jour** et donnent lieu à application du tiers-payant, la convention nationale organisant les rapports entre les médecins libéraux et l'assurance maladie, en vigueur depuis 2016²⁶, prévoit que le médecin est malgré tout rémunéré par le régime d'assurance maladie obligatoire, quels que soient le régime d'affiliation du patient et sa caisse de rattachement.

Lors de l'établissement de la FSE, le paiement reste également garanti si le professionnel de santé utilise le service ADRI (acquisition des droits intégrée), **avec la carte Vitale du patient**, pour obtenir une situation à jour de ses droits depuis les bases de l'Assurance Maladie. À titre d'exemple, si la prise en charge à 100 % n'apparaît pas encore sur la carte Vitale du patient, la consultation d'ADRI, permet au professionnel de santé de s'assurer de la validité d'une prise en charge à 100 % et de l'appliquer en lieu et place du niveau de prise en charge de 70 % encore inscrit sur la carte Vitale du patient.

1.2.3. Une infrastructure composée de 410 000 terminaux de lecture des cartes et de logiciels déployés chez les professionnels de santé est régulée et homologuée par le GIE SESAM-Vitale et la CNDA

Le **déploiement de l'infrastructure de lecture des cartes Vitale** chez les professionnels de santé et dans les établissements a constitué le pendant de la diffusion du parc de cartes Vitale chez les assurés. Au fil des évolutions, le marché des lecteurs s'est ouvert afin de réduire les coûts d'équipement et simplifier les usages.

Au fil des évolutions d'homologation, l'accès à du matériel standardisé, moins coûteux, s'est élargi :

- ◆ **lors de la mise en place du programme SESAM-Vitale**, le GIE SESAM-Vitale a, dans premier temps, lancé un appel d'offres pour des lecteurs de cartes Vitale (et CPS) afin d'équiper les premiers professionnels de santé utilisant des logiciels de facturation conforme au cahier des charges SESAM-Vitale ;
- ◆ **à partir des années 1999-2000**, le GIE SESAM Vitale a ouvert le marché des lecteurs de carte Vitale à tous les industriels en publiant un **référentiel d'homologation SESAM-Vitale de lecteur de cartes Vitale (et CPS)**²⁷ ;
- ◆ **depuis 2014**, les logiciels des professionnels de santé conformes au cahier des charges SESAM-Vitale peuvent aussi utiliser des **lecteurs de cartes dit standard appelés PC/SC ou transparents** pour lire les cartes Vitale : cette option est devenue obligatoire depuis 2018 pour toutes les nouvelles versions des logiciels des professionnels de santé. Ce choix permet d'envisager des évolutions technologiques sans nécessiter le changement du parc de lecteurs.

En juin 2022, sur un parc d'environ 410 000 lecteurs utilisés en facturation SESAM-Vitale :

- ◆ 15% étaient des lecteurs standard PC/SC ;
- ◆ 54% des lecteurs bi-mode homologués SESAM-Vitale et standard PC/SC ;
- ◆ 31% des lecteurs SESAM-Vitale ancienne génération.

²⁶ Arrêté du 20 octobre 2016 portant approbation de la convention nationale organisant les rapports entre les médecins libéraux et l'assurance maladie signée le 25 août 2016.

²⁷ Le centre national de dépôt et d'agrément (CNDA), service de l'Assurance Maladie, certifie depuis 1998 les logiciels des éditeurs partenaires avec l'agrément des logiciels de facturation sécurisée pour lesquels il est nécessaire de garantir la conformité au cahier des charges SESAM-Vitale et à ses additifs.

Annexe I

Les lecteurs permettant l'**authentification hors ligne** de la carte Vitale 2 (voir *infra*) permettent de réaliser des feuilles de soins électroniques en visite (actes isolés), de les enregistrer puis de les transférer vers l'ordinateur du cabinet pour les transmettre vers l'assurance maladie.

Le déploiement de ces lecteurs hors ligne chez les professionnels de santé a été très fort ces dernières années, pour atteindre 92,7 % du parc installé en 2021 (contre 86,9 % en 2020).

En 2021, il ne restait pour toute la France que 2 professionnels équipés d'un lecteur 2.0, rendus inutilisables pour l'émission de FSE depuis juin 2022 (cf. tableau 3).

Le nombre de professionnels de santé équipés de lecteurs dits transparents (PC/SC) est passé de 33 651 fin 2020 à 69 896 en 2021, soit + 52 % en un an.

Tableau 3 : Composition du parc de lecteurs de cartes Vitale

Types de lecteurs de carte Vitale	Nombre	Part du parc
Lecteurs permettant l'authentification hors ligne	366 179	92,7%
<i>dont nombre de PS28 équipés de lecteurs 3.30</i>	<i>128 764</i>	<i>32,6%</i>
<i>dont nombre de PS équipés de lecteurs 4.0</i>	<i>167 519</i>	<i>42,4 %</i>
<i>dont nombre de PS équipés de lecteurs PC/SC</i>	<i>69 896</i>	<i>17,7 %</i>
Autres lecteurs	28 933	7,3%

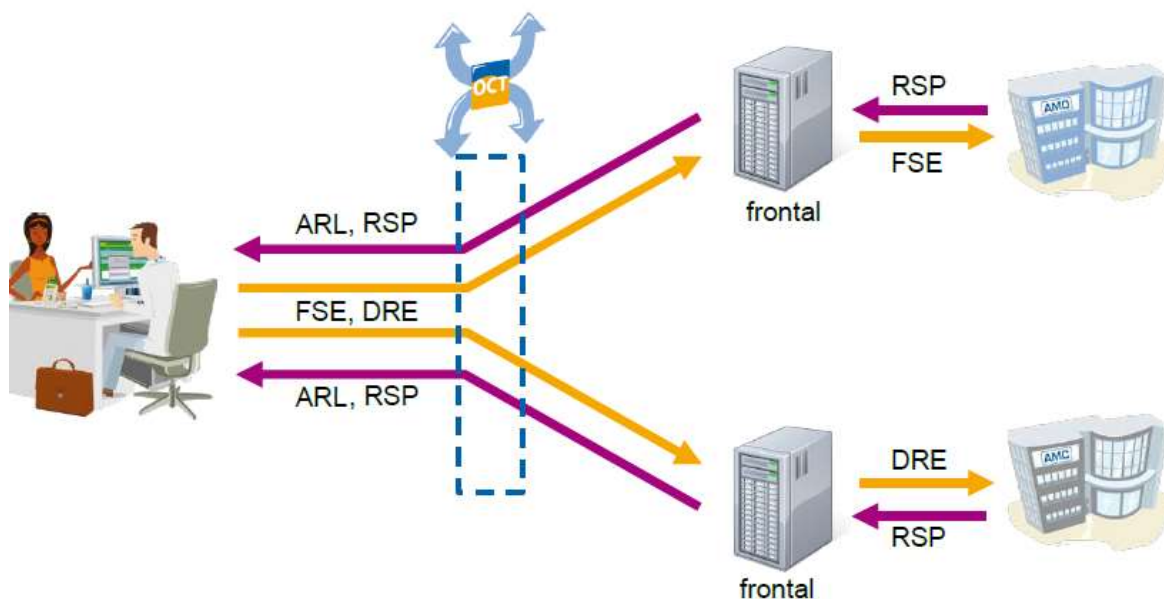
Source : GIE SESAM-Vitale.

En parallèles des flux de FSE, le service de **demande de remboursement électronique (DRE)** des FSE permet un envoi direct des demandes **aux organismes d'assurance maladie complémentaire (AMC)**. Ce système de facturation est conçu et mis à jour par le GIE SESAM-Vitale et intervient en parallèle de l'envoi des FSE aux frontaux de facturation²⁹ des organismes d'assurance maladie obligatoire (cf. Graphique 1). Le paiement est garanti au professionnel de santé dans un délai de quatre jours ouvrés.

²⁸ Professionnels de santé.

²⁹ Progiciel conçu, réalisé et édité par le GIE SESAM-Vitale et mis à disposition de prestataires afin de permettre la réception, le contrôle et le routage des flux SESAM-Vitale dans l'objectif unique de liquidation des prestations à destination des organismes AMO et AMC .

Graphique 1 : Schéma des flux de facturation dématérialisés (FSE et DRE)



Source : GIE SESAM Vitale.

2. S'appuyant sur diverses évolutions technologiques, le parc de cartes Vitale fait l'objet d'une gestion renforcée depuis 2004 avec la mise en place de listes d'opposition mises à jour quotidiennement

2.1. La modernisation du parc de cartes Vitale a répondu à des enjeux de sécurité et à une volonté d'élargir les informations inscrites sur la carte

2.1.1. Les fonctionnalités et les données contenues sur la carte Vitale ont peu évolué depuis sa mise en place, malgré le déploiement à partir 2007 de la carte Vitale 2 dotée d'une photographie de l'assuré

Depuis son introduction, **la carte Vitale a régulièrement évolué pour prendre en compte des évolutions technologiques et cryptographiques.**

Suite à l'adoption de la loi du 13 août 2004³⁰, qui a rendu obligatoire la présence de la photographie de l'assuré sur la carte Vitale, **les cartes émises depuis le 1er décembre 2007 sont désignées comme « cartes Vitale 2 »**³¹. Depuis cette date, les organismes ne peuvent délivrer à leurs bénéficiaires que des cartes Vitales dotées d'une photographie.

Ainsi, **les puces de cartes Vitale 1 (émises avant 2007) et cartes Vitale 2**, qui composent l'ensemble du parc de cartes Vitale actuellement en circulation (cf. *infra*) **contiennent obligatoirement les informations suivantes :**

³⁰ Article L. 161-31 du code de la santé publique

³¹ Le décret n° 2007199 du 14 février 2007 relatif à la carte d'assurance maladie et modifiant le code de la sécurité sociale réglemente la diffusion des cartes Vitale 2. Il prévoit que : « *chaque organisme servant les prestations d'un régime d'assurance maladie délivre une carte d'assurance maladie aux personnes qui lui sont rattachées, en s'assurant de l'identité du titulaire de la carte. La carte d'assurance maladie est la propriété de l'organisme servant les prestations d'un régime d'assurance maladie. Lors de la mise à disposition d'une carte d'assurance maladie, l'organisme d'affiliation vérifie que le titulaire de la carte n'est possesseur d'aucune autre carte valide* ».

Annexe I

- ◆ l'identité du porteur (nom, prénoms, date de naissance) et celle de ses ayants-droits, défini comme une personne qui tient son droit à l'assurance maladie du fait de ses liens avec un assuré de plus de 16 ans ;
- ◆ son numéro de sécurité sociale (NIR) ;
- ◆ le régime d'assurance maladie et l'organisme auquel est rattaché l'assuré ;

Le cas échéant, les cartes Vitale peuvent également contenir des **informations relatives à la situation de l'assuré** :

- ◆ les éventuels droits à la complémentaire santé solidaire (CSS) ;
- ◆ l'existence d'une **affection de longue durée (ALD), sans précision de sa nature** ;
- ◆ **le bénéfice du régime de maternité** ;
- ◆ **le bénéfice du régime des accidents de travail ou des maladies professionnelles** ;

Ces informations figurent en carte afin de permettre à l'assuré social de bénéficier des exonérations de ticket modérateur ou de dispense d'avance de frais auxquelles il a droit, selon sa situation.

Les cartes Vitale de deuxième génération (Carte Vitale 2), mises en circulation en 2007, comportent une photographie de l'assuré, qui figure au recto de la carte et doit correspondre aux spécifications de la norme « ISO/IEC 19794-5:2005 », identique à celle des cartes d'identité et passeports. Elle est également inscrite sur la puce de la carte, mais non accessible et avec une définition trop faible pour un usage biométrique³² (77 x 97 pixels pour 4 096 octets au maximum).

La carte Vitale 2 permet également d'accueillir des informations qui ne figurent pas sur la carte Vitale de première génération, notamment sur la **complémentaire santé de l'assuré** :

- ◆ mention du médecin traitant déclaré ;
- ◆ mention d'une éventuelle mutuelle santé ;
- ◆ personne à prévenir en cas de nécessité ;
- ◆ accès aux soins dans l'Union européenne ;
- ◆ gestion des accidents du travail et des maladies professionnelles ;
- ◆ mention indiquant que son titulaire a eu connaissance des informations sur le don d'organes.

La carte Vitale dispose d'un composant électronique contenant l'ensemble de ces informations ainsi que des **données relatives à la carte elle-même** :

- ◆ un numéro d'émetteur,
- ◆ un numéro propre à la carte ;
- ◆ la date de son émission.

Les informations stockées dans la carte sont donc de nature administrative (état-civil, NIR, médecin traitant, caisse de rattachement, bénéfice de la CSS, données de gestion de la carte etc...) **à l'exception de deux données particulières** :

- ◆ **l'existence d'une affection de longue durée** pourrait constituer une donnée médicale. Toutefois, le numéro de l'ALD n'étant pas stocké en carte, il n'est pas possible de connaître la pathologie précise de son porteur, les ALD couvrant un large spectre de maladies chroniques (CSS, art. D. 160-4). Les professionnels de santé doivent recourir à d'autres outils (par exemple Ameli Pro) pour connaître la nature exacte de l'ALD ;
- ◆ **l'existence d'une grossesse.**

La carte Vitale ne comporte donc pas de donnée de santé au sens strict du terme.

³² Cf. annexe V relative à la biométrie.

Encadré 6 : Les données de santé au sens du règlement européen sur la protection des données personnelles RGPD

Pour mémoire le règlement européen sur la protection des données personnelles (RGPD), qui est entré en application le 25 mai 2018 procède à une définition large des données de santé.

Les données à caractère personnel concernant la santé sont les données relatives à la santé physique ou mentale, passée, présente ou future, d'une personne physique (y compris la prestation de services de soins de santé) qui révèlent des informations sur l'état de santé de cette personne. Cette définition comprend donc par exemple :

- les informations relatives à une personne physique collectées lors de son inscription en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services : un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé ;
- les informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir des données génétiques et d'échantillons biologiques ;
- les informations concernant une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée (indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic in vitro).

Source : Mission.

Enfin, la carte Vitale permet au professionnel de santé d'accéder à des informations sur **l'historique des consommations du patient et de ses prises en charge par l'assurance maladie**. Les médecins peuvent ainsi, à l'occasion des soins qu'ils délivrent³³ consulter ces données détenues par l'organisme dont relève chaque bénéficiaire de l'assurance maladie. Dans ce cas, ils en informent préalablement le patient.

Le **relevé des données mis à la disposition du médecin** contient :

- ◆ les informations nécessaires à **l'identification des actes, produits ou prestations pris en charge pour les soins** délivrés en ville ou en établissement de santé, au regard notamment des listes mentionnées aux articles L. 162-1-7, L. 165-1 et L. 162-17 ;
- ◆ le code prévu pour les identifier dans ces listes ;
- ◆ le **niveau de prise en charge** ;
- ◆ pour les patients atteints d'une affection de longue durée (ALD), les éléments constitutifs du protocole de soins mentionné au septième alinéa de l'article L. 324-1.

Il ne contient aucune information relative à l'identification des professionnels de santé prescripteurs.

2.1.2. La sécurisation des données contenues dans la carte a nécessité diverses évolutions techniques depuis 1998

Afin de sécuriser les informations portées par la carte Vitale, le GIE SESAM Vitale s'est appuyé sur la technologie issue du secteur bancaire et a fait évoluer le programme fonctionnel et les algorithmes cryptographiques qui protègent les données inscrites en carte. **Quatre générations de carte ont ainsi été émises :**

- ◆ deux versions de la **carte Vitale 1** :
 - **Entre 1998 et 2003**, la **carte Vitale 1 « SCOT »** disposait d'un programme fonctionnel, ou masque, « M9 » conforme à la norme française des cartes bancaires

³³ Sous les conditions prévues à l'article L. 161-31 du code de la sécurité sociale.

Annexe I

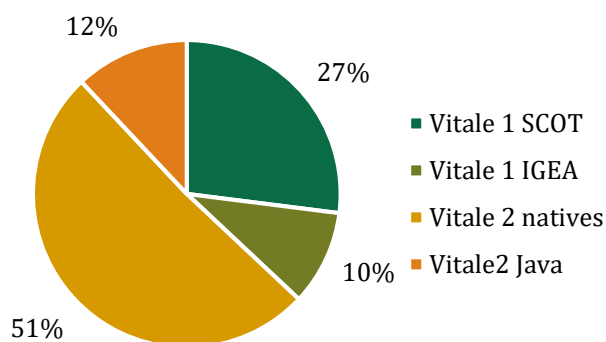
établie dans les années 1980. La sécurisation des données figurant sur la carte était assuré initialement par l'algorithme cryptographique DES³⁴, utilisé pour l'authentification de la carte et le scellement de documents ;

- **de 2003 à 2007**, l'algorithme DES a été remplacé par l'algorithme 3DES³⁵, sur la **carte Vitale 1 « IGEA »** ;
- ◆ deux versions de la **carte Vitale 2** :
 - **entre 2007 et 2019**, la carte Vitale 2 associée à un algorithme 3DES, dite **carte Vitale 2 native**, a été diffusée en employant les algorithmes cryptographiques 3DES, puis RSA³⁶ (2048 bits) et SHA-1³⁷ ;
 - **depuis 2019**, le masque est implémenté sur composant JavaCard, et les algorithmes cryptographiques ont été modernisés : AES³⁸, RSA (2048 bits) et SHA-2³⁹.

Au 31 décembre 2021, le parc de cartes Vitale était constitué de 57,9 millions de cartes valides, dont :

- ◆ **21,2 millions de cartes Vitale 1, donc ne comprenant pas de photographie de l'assuré, soit 36,6 % du parc :**
 - 15,5 millions de cartes SCOT ;
 - 5,7 millions de cartes IGEA ;
- ◆ **36,7 millions de cartes Vitale 2, soit 63,4 % du parc :**
 - 29,4 millions de cartes V2-natives ;
 - 7,3 millions de cartes V2-Java émises à partir de juin 2019.

Graphique 2 : Composition du parc de cartes Vitale en 2021, par génération de masque (en %)



Source : Suivi technique Parc Cartes Vitale, 2021, GIE SESAM-Vitale.

³⁴ Data Encryption Standard : standard de chiffrement datant de 1977 et utilisant des clés de chiffrement de 56 bits. Le simple DES est aujourd'hui considéré comme obsolète.

³⁵ Triple DES : application de l'algorithme DES avec successivement trois clés de chiffrement différentes.

³⁶ Technique de chiffrement brevetée en 1983. RSA représente les initiales des inventeurs : Rivest, Shamir et Adleman.

³⁷ Secure Hash Algorithm, version 1, datant de 1995. Les principaux navigateurs n'acceptent plus les certificats SHA-1, en raison de sa faible sécurité.

³⁸ Advanced Encryption Standard, datant de 2000.

³⁹ SHA de deuxième génération (datant de 2001). Cette génération améliore très sensiblement la sécurité par rapport à SHA-1.

Annexe I

À l'émission des nouvelles cartes, leur sécurité est évaluée selon les critères communs et **qualifiée au niveau EAL4+⁴⁰ par l'Agence nationale de la sécurité des systèmes d'information (ANSSI)**, d'un niveau de sécurité équivalent aux cartes bancaires. Il s'agit du niveau de sécurité le plus élevé pour des applications civiles.

Le niveau de sécurité est ensuite contrôlé au long de la vie des cartes sur le terrain lors d'études de vieillissement pilotées par le GIE SESAM-Vitale.

Les clés cryptographiques sont établies selon un schéma à trois niveaux :

- ◆ clés «grand-mères», sauvegarde stockée en banque ;
- ◆ clés «mères», changées tous les millions de cartes ;
- ◆ clés «filles» ou clés «cartes» uniques par cartes.

Constitué de 15 socles techniques différents⁴¹, le parc est donc **très hétérogène** sans toutefois présenter « *de risque majeur* », selon le GIE SESAM-Vitale.

Selon le GIE SESAM-Vitale, **les technologies les plus anciennes équipées de composants SCOT (20 à 24 ans d'âge), sont devenues fragiles**, et notamment les technologies Sc1 et Sc4 (soit environ 7,8 millions de cartes fin 2022). Toutefois le risque associé au cassage de l'algorithme de chiffrement de ces cartes est plus un risque en termes de notoriété et d'image que de fraude, puisqu'il revient à rendre disponible à la lecture les données contenues en carte.

Seule, la technologie la plus récente « Ja1 », émise depuis juin 2019 en Javacard, n'a pas été testée dans le cadre d'une étude 'vieillissement' par le GIE SESAM-Vitale.

2.2. Un processus de production des cartes Vitale maîtrisé par le GIE SESAM-Vitale pour un coût de production et de gestion s'élevant à 2,63€ par carte Vitale

2.2.1. Le GIE SESAM-Vitale conçoit et produit environ 4 millions de cartes Vitale par an pour le compte de ses membres.

Entre 2019 et 2022, le rythme de production a été stable : **3,9 millions de cartes Vitale ont été produites en 2021 et 2022**, proche des 4 millions de cartes Vitale produites en 2019. En 2020, la crise sanitaire explique en partie la baisse de 300 000 unités produites (3,6 millions de cartes produites).

Tableau 4 : Nombre de cartes Vitale produites par le GIE SESAM-Vitale, entre 2019 et 2022 (en millions)

Année	Nombre de cartes Vitale produites (en millions)
2019	4,0
2020	3,6
2021	3,9
2022	3,9

Source : GIE SESAM-Vitale

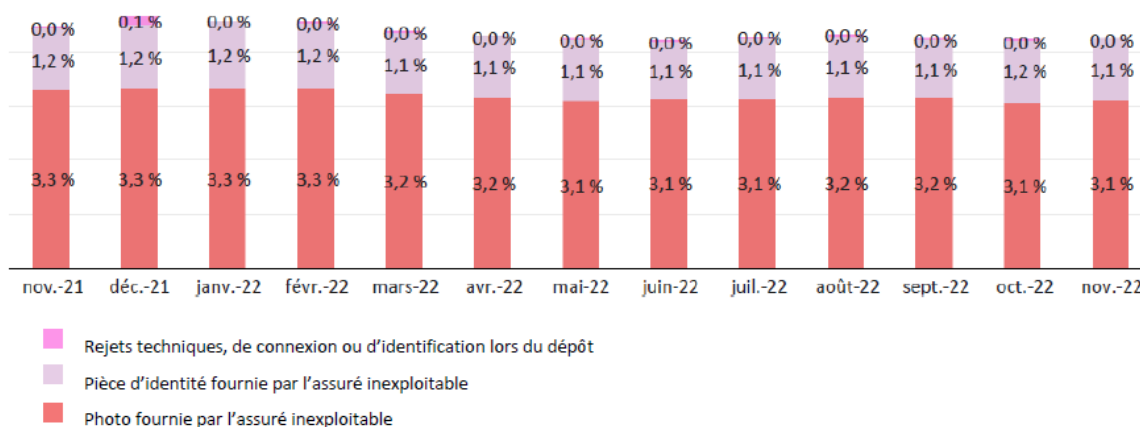
⁴⁰ Évaluation Assurance Level, dont le niveau de sécurité est classé de 1 (test le moins complet) à 4+ (test le plus complet).

⁴¹ Huit technologies pour les cartes Vitale 1 et sept technologies pour les cartes Vitale 2.

Le **GIE SESAM-Vitale sous-traite la numérisation de la photo des cartes Vitale** à un industriel, appelé numériseur, qui reçoit soit les plis papier avec la photo et la photocopie de la pièce d'identité de l'assuré envoyés via la poste par l'assuré, soit la photo numérisée et le scan de la pièce d'identité déposés par l'assuré sur le portail de l'assurance maladie (par exemple ameli.fr ou msa.fr).

Bien que les standards requis par l'assurance maladie pour accepter la photographie d'identité soient plus souples que ceux exigés pour la délivrance d'un titre sécurisé, un nombre non négligeable de demandes ne sont pas exploitables faute de photographie de qualité suffisante, ce qui rallonge les délais de fabrication de la carte en question et peut nécessiter un déplacement de l'assuré au guichet de sa caisse primaire. D'après le GIE SESAM Vitale, la transmission d'une photographie inexploitable est la première cause de rejet, loin devant la pièce d'identité. Les deux motifs principaux sont un problème de détection du visage sur la photo ou un autre défaut de la photo, tel qu'un problème de luminosité⁴².

Graphique 3 : Taux de dépôts numériques inexploitables, par origine (novembre 2021-novembre 2022)



Source : GIE SESAME Vitale, tableau de bord tous régimes, novembre 2022.

Le numériseur vérifie ensuite la correspondance entre la photo et la pièce d'identité, et entre la pièce d'identité et l'identité connue dans les bases de l'assurance maladie, puis garde la photo validée à disposition pour la production de la carte. Le GIE SESAM-Vitale développe et opère le système d'information permettant d'interfacer le numériseur et les différents régimes d'assurance maladie obligatoire.

Par ailleurs, le **GIE SESAM-Vitale établit les spécifications de la carte Vitale**, puis sous-traite leur conception et leur production à un industriel de la carte à puce.

L'industriel conçoit la carte Vitale, la fait certifier et qualifier d'un point de vue sécurité, puis met en place les chaînes de production du module électronique de la carte, de la carte vierge composée de son support plastique et du module, et de personnalisation de la carte permettant d'y insérer les informations personnelles d'un assuré.

Le GIE SESAM-Vitale passe ensuite des commandes de cartes vierges en fonction d'estimations prévisionnelles établies avec les régimes d'assurance maladie obligatoire.

⁴² Les rejets sont dus à diverses raisons : photo inexploitable par manque de luminosité, ou floue, comprenant des défauts de cadrage, le port de couvre-chefs, des motifs en arrière-plan, des taches ou des rayures... Source : GIE SESAM Vitale, tableau de bord tous régimes, novembre 2022.

Annexe I

Le GIE SESAM-Vitale développe et opère un **système d'information permettant d'interfacier les régimes d'assurance maladie obligatoire avec les ateliers de personnalisation** (de l'industriel de la carte à puce et de celui de la Cnam). Les régimes d'assurance maladie passent des ordres de personnalisation des cartes et les industriels renvoient des comptes rendus de production une fois les cartes personnalisées envoyées aux assurés par voie postale.

2.2.2. Le coût total de production d'une carte Vitale est de 2,63 €

En 2021, le coût de production industrielle d'une carte Vitale était de 2,07 € (0,38 € de numérisation de la photo, 0,52 € pour la carte vierge, 0,62 € pour la personnalisation, et 0,54 € pour le timbre de l'envoi de carte Vitale à l'assuré). **Les coûts de gestion du GIE SESAM-Vitale s'élevaient à 0,56 € par carte Vitale émise.**

Le coût total de production d'une carte Vitale pour le GIE SESAM-Vitale est donc de 2,63 €. Ces coûts ne comprennent pas les coûts de gestion des régimes d'assurance maladie.

Les délais de production d'une carte Vitale étaient de 10 jours en novembre 2022. Il s'agit du délai de production global mesuré pour toutes les cartes Vitale produites dans le mois entre la date d'entrée du formulaire chez le numériseur et la date de remise à la poste de la carte par les ateliers de personnalisation (cf. tableau 5). Les délais présentés dans le tableau sont calculés carte à carte pour chaque processus. Les délais moyens de chaque processus ne sont donc pas cumulables.

99% des cartes Vitale étaient produites dans un délai de sept jours ouvrés en novembre 2022 (en juin et septembre 2022, ce délai était réduit à 3 jours ouvrés).

Tableau 5 : Décomposition du délai moyen de production d'une carte Vitale en novembre 2022 (en jours)

Étape de production	Processus (initial/final)	Délai moyen
Numériseur	Entre la date d'entrée du formulaire chez le numériseur et la mise à disposition de la photo (et délai avis caisse pour les cas nécessitant un avis de la caisse)	4 jours
AMO	Entre la date de mise à disposition de la photo et la date de demande de production de l'AMO reçue par le PEC.	3,1 jours
PEC	Entre la date de demande de production de l'AMO et la date d'envoi de la demande aux ateliers (à un rythme quotidien). Il inclut la réponse du RNIAM aux contrôles de cohérence ainsi que la réponse du numériseur à la demande photo.	ND
Ateliers	Entre la date d'envoi de la demande aux ateliers et la date de remise de la carte à la poste :	4,4 jours

Source : GIE-SESAM-Vitale ; mission.

Pour mémoire, les **trois scénarios de création de carte sont** :

- ◆ la primo-émission d'une carte Vitale pour un assuré n'en ayant jamais possédé (20% des cas) ;
- ◆ l'émission sans doublon, pour un assuré ayant déjà eu une carte Vitale, mais ne disposant d'aucune carte valide au moment de la production de la nouvelle carte Vitale (69% des cas) ;
- ◆ l'émission avec doublon pour un assuré disposant d'une carte Vitale valide au moment de la production de la nouvelle carte Vitale (11% des cas) ;

2.3. Le parc de carte Vitale comptait 57,9 millions de cartes valides au 31 décembre 2021, dont 64% de cartes Vitale 2 porteuses de la photo de l'assuré

Au 31 décembre 2021, le GIE SESAM-Vitale faisait état de 57,9 millions de cartes valides, soit 0,33 million en moins par rapport à 2020.

Le parc de cartes Vitale comprenait 29,3 millions de cartes ayant 10 ans ou plus (50,6 %), dont 11,6 millions datant du déploiement initial en 1998-1999 (20,0 %).

Au cours de l'exercice 2021 :

- ◆ 3,87 millions de cartes Vitale 2 ont été émises ;
- ◆ 2,58 millions de cartes ont été mises en fin de vie, dont 0,96 million de cartes Vitale 1 ;
- ◆ 51,7 millions de cartes ont été mises à jour.

Tableau 6 : Situation des cartes Vitales émises depuis 1998, en date du 31 décembre 2021

Situations ⁴³	Parc Global	Vitale 1	Vitale 2
Cartes émises depuis 1998	154,7	97,7	57,1
Cartes détruites	41,7	34,8	6,9
Cartes invalidées non détruites	4,7	2,9	1,8
Cartes en fin de vie en LOD	50,4	38,7	11,7
Cartes valides	57,9	21,2	36,7
Nombre de porteurs estimé au 31/12/2021 *	60,1		

La maîtrise du parc de cartes Vitale, tant sur les cartes déployées aux personnes que sur la conformité des données de la carte par rapport aux fichiers des organismes d'assurance maladie obligatoire, est un enjeu important pour l'assurance maladie et un élément incontournable de lutte contre la fraude. (cf. annexe III).

2.4. Une faiblesse structurelle du dispositif est liée à son architecture locale et à l'impossibilité de mettre à jour systématiquement les droits inscrits en carte, emportant un préjudice financier potentiellement important pour l'assurance maladie

La carte Vitale contient les informations relatives au détenteur et à ses droits. Ces données étant inscrites localement sur la carte, elles peuvent ne plus être à jour en cas de changement de situation de l'assuré social (déménagement entraînant un changement de caisse, ALD, changement de médecin traitant, changement d'organisme assurant la prise en charge des frais de santé).

Afin de limiter les écarts entre les droits ouverts et ceux portés par la carte Vitale, il est prévu une obligation de mise à jour, à la charge de l'assuré social⁴⁴, annuelle ou lors d'un changement de situation personnelle⁴⁵. Cette mise à jour est à effectuer en pharmacie ou sur les bornes

⁴³ *Ce nombre est une estimation qui provient de la CNAV transmis, données du 01/01/2022. Ce nombre est obtenu en retenant uniquement les bénéficiaires certifiés rattachés au RNIAM (Registre National Inter-Régimes des bénéficiaires de l'Assurance Maladie) non décédés, et âgés de 16 ans et plus.

⁴⁴ CSS, art. R. 161-30-10.

⁴⁵ Article R. 161-33-10 du code de la sécurité sociale.

Annexe I

mises à disposition dans les caisses primaires d'assurance maladie ainsi que dans certains établissements de santé⁴⁶.

En pratique, cette opération est effectuée en moyenne 1,2 fois par an⁴⁷. Toutefois il subsiste une partie importante du parc dont les cartes ne sont pas mises à jour (cf. *infra*).

Or, que les droits en carte aient été ou non actualisés, les professionnels de santé bénéficient d'une garantie de paiement des droits inscrits sur la puce. Cela peut amener les régimes d'assurance maladie à supporter un préjudice financier dont le montant est potentiellement substantiel mais que l'assurance maladie n'est pas en capacité de chiffrer et que les estimations de la mission n'ont pas permis de préciser (cf. annexe IV relative à l'application carte Vitale).

2.4.1. Depuis 2019, environ 80 % des cartes Vitale font l'objet d'une mise à jour annuelle

Au cours de l'année 2021, 79,7 % des cartes Vitale valides ont été mises à jour. Le taux de mise à jour était en baisse de 2,5 points par rapport à l'année 2020 (82,2 %). **Ce sont donc 20% de cartes valides qui n'avaient pas été mises à jour en 2021**, ne serait-ce qu'une seule fois dans l'année⁴⁸. Ce chiffre diminue dans le temps.

À fin 2022, plus d'un million de cartes n'avaient pas été mises à jour depuis plus de deux ans (cf. tableau 7). Pour une partie non négligeable du parc de cartes, les droits ainsi contenus en carte ne sont donc pas à jour lorsque la carte Vitale est présentée au professionnel de santé en ville pour la facturation d'un acte.

Tableau 7 : Nombre de cartes valides (en circulation) sans mise à jour depuis plus de deux ans⁴⁹

Délai de non mise à jour	Nombre de cartes Vitales valides
Sans télémise à jour depuis 6 ans	128985
Sans télémise à jour depuis 6 ans	194866
Sans télémise à jour depuis 6 ans	303014
Sans télémise à jour depuis 6 ans	539254
Sans télémise à jour depuis 6 ans	1074058

Source : GIE SESAM-Vitale. ; cartes Vitale émises avant 2022 et valides au 30 novembre 2022.

Suite aux opérations de nettoyage du parc de cartes Vitale entamées en 2017, **le taux de mise à jour du parc ne varie plus en fonction de l'année de personnalisation de la carte.** En particulier, à partir de **2021**, on constate une répartition homogène des mises à jour en fonction de l'année de personnalisation de la carte (cf. graphique 4).

À titre de comparaison, en 2017, **la part du parc de cartes valides mise à jour au cours de l'année était d'un niveau plus faible (73,8%)**. Le taux de mise à jour du parc variait alors en fonction de l'année de personnalisation de la carte du fait de cartes anciennes, personnalisées au début des années 2000 et considérées comme valides à tort.

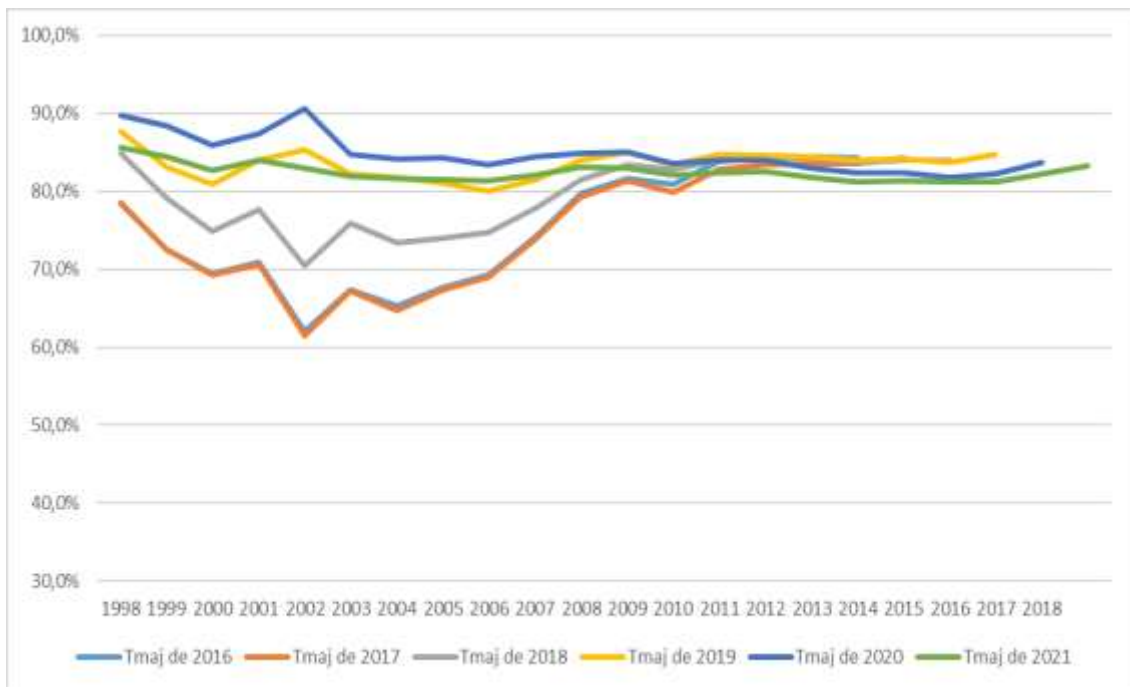
⁴⁶ Les pharmaciens sont incités moyennant rémunération sur objectif de santé public (ROSP) à procéder à la mise à jour des cartes Vitale (sous réserve de l'accord des assurés). Ils disposent du matériel nécessaire en lecture / écriture (soit environ 100 000 terminaux) pour modifier les données stockées sur la carte Vitale, contrairement aux autres professionnels de santé (sauf exceptions).

⁴⁷ Source : GIE SESAM Vitale

⁴⁸ Source : GIE SESAM Vitale. 2021-CMS VITALE TOUS REGIMES-v1.00

⁴⁹ Q01-T02-01-Cartes_Vitale_valides_par_année_de_dernière_télémise_à_jour_-_v1

Graphique 4 : Taux de mise à jour du parc de carte Vitale en fonction de l'année de personnalisation (données 2021)



Exemple de lecture : en 2017, 60% des cartes valides émises en 2002 ont été mises à jour.

Source : GIE SESAM-Vitale

En 2021, 0,89 million de cartes Vitale ont été invalidées à l'occasion d'une opération de mise à jour contre 0,82 million en 2020, année marquée par la crise sanitaire (accueils des caisses fermés et assurés confinés).

2.5. Un système d'opposition a été mis en place à partir de 2004 afin d'améliorer la gestion du parc de cartes Vitale et de répondre aux besoins des différents acteurs du système de santé

2.5.1. Le système repose sur la base de gestion technique des cartes (GTC) gérée par le GIE SESAM Vitale qui permet d'établir des listes d'opposition diffusées aux acteurs de santé en fonction de leurs besoins

Un système d'opposition des cartes Vitale a été mis en place par le GIE SESAM-Vitale à partir de 2004, soit six ans après le déploiement des premières cartes Vitale, alors que la possibilité d'établir un tel système était prévue dès 1998 par voie réglementaire⁵⁰.

Une carte Vitale en opposition est une carte dont l'utilisation est interdite :

- ◆ parce qu'elle a été déclarée **perdue** ou **volée** ;
- ◆ ou parce que le **régime d'assurance maladie obligatoire de l'assuré l'a dénoncée** (pour défaut de mise à jour de droits particuliers par exemple).

⁵⁰ Décret n°98-275 du 9 avril 1998.

Annexe I

Le système d'opposition s'appuie sur les **informations contenues dans la base de données de gestion technique des cartes (GTC) qui répertorie l'ensemble des numéros de série des cartes Vitale inter-régimes** qui ne doivent pas être utilisées sur les postes des professionnels de santé, ni en facturation, ni en téléservices. Elle comprend l'ensemble des cartes Vitale qui y ont été placées depuis sa création en 2004.

Les données d'opposition sont mises à jour quotidiennement dans un **double objectif** :

- ◆ empêcher toute utilisation, en facturation et en téléservices, des cartes Vitale qui ont été mises en fin de vie ;
- ◆ réduire la mobilisation de la garantie de paiement au bénéfice des professionnels de santé. En effet, si la carte Vitale n'a pas été mise à jour, elle peut être porteuse de droits dont l'assuré n'est plus bénéficiaire, notamment le tiers payant pour tout ou partie des soins reçus.

À titre d'exemple, sur la base des informations inscrites sur la carte Vitale, un professionnel de santé peut être dans l'obligation de dispenser le patient de toute avance des frais. Or, si les informations sont erronées du fait d'une absence de mise à jour de la carte Vitale, **le flux de facturation émis par le professionnel de santé sera rejeté** par le régime d'assurance maladie obligatoire. **L'utilisation de la carte Vitale permet toutefois au professionnel de santé de bénéficier d'une garantie de paiement.** Même sans droits (tiers-payant) l'assurance maladie assure le règlement des factures émises par les professionnels de santé.

Le GIE SESAM-Vitale a mis en place un système appelé **Gestion Technique des Cartes (GTC) qui recouvre le suivi du parc de cartes Vitale et l'exécution des marchés** passés entre le GIE SESAM Vitale et les industriels désignés comme « personnalisateurs », en charge d'intégrer les données des assurés sur les cartes Vitale.

La base de données GTC exploitée par le GIE SESAM-Vitale est alimentée par :

- ◆ les **fichiers GTC**, constitués à partir des fichiers envoyés par les industriels lors de la personnalisation des cartes ;
- ◆ les **fichiers FEC** (fichier événements cartes), transmis par les régimes d'assurance maladie, comportent les informations de fin de vie des cartes, de mutation et les informations relatives au traitement

Par ailleurs, la base GTC intègre également **deux types de fichiers concernant la production des cartes Vitale** :

- ◆ les **fichiers descendants**, établis par les centres de traitement informatique (CTI) suite aux phases de sélection et de personnalisation, comportent les **données qui figureront sur la carte**, à la fois dans la puce et sur le recto de la carte (sérigraphie) et sur la lettre d'accompagnement (attestation de personnalisation) ;
- ◆ les **fichiers remontants**, transmis par les industriels personnalisateurs (cf. *supra*) **après production des cartes Vitale** pour mise à jour de la base de données «cartes» du CTI qui a produit le fichier descendant correspondant. Les fichiers remontants comportent notamment le numéro de série des cartes produites et leur date de fabrication.

Ce **système de double fichier**, descendant et remontant, permet de sécuriser la phase de production et d'éviter l'utilisation d'une carte Vitale avant que le processus de création de la carte ne soit achevé. Ainsi, lorsque le fichier remontant n'est pas encore traité au niveau du CTI ayant émis le fichier descendant, et que les cartes figurant sur le fichier sont utilisées pour réaliser des feuilles de soin électroniques (FSE), ces dernières sont rejetées lors de leur traitement par l'assurance maladie (« rejet n° 9080 036 : carte Vitale inexistante »).

La GTC reçoit deux catégories d'**événements** :

- ◆ les événements d'opposabilité ;
- ◆ les événements de fin de vie.

Annexe I

À partir des données remontées en continu à la base GTC, il est possible de constituer des fichiers destinés aux divers usagers et professionnels de santé :

- ◆ les fichiers constituant des **listes d'opposition** (cf. *infra*) ;
- ◆ les fichiers AEC (avis évènement cartes) qui **informent les régimes** :
 - de la **destruction physique des cartes** par le Centre des retours cartes ;
 - du résultat de l'**expertise des cartes défectueuses** ;
 - des **clôtures des mutations** des cartes Vitale.

Tableau 8 : Motifs de mise en fin de vie des cartes Vitale

Code événement de fin de vie	Libellé
01	Carte perdue ou volée.
02	Carte en incident.
03	Carte frauduleuse.
04	Carte présumée abusive.
05	Carte abusive.
06	Porteur décédé.
08	Changement de visuel.
09	Mutation carte échouée.
11	Carte non mutée dans les délais impartis.
12	Valide bénéficiaire non repris par régime absorbant.
13	Carte frauduleuse opposable.
14	Carte abusive opposable.
17	Carte frauduleuse opposable à nouveau utilisée.
18	Carte abusive opposable à nouveau utilisée.
27	Carte renouvelée.
30	Carte en doublon.
31	Carte en double.
71	Carte invalidée par SIMS.
99	Indéterminé.

Source : GIE Sesam-Vitale.

2.5.2. Trois listes d'opposition sont constituées pour répondre aux besoins des professionnels de santé et des régimes d'assurance maladie

Initialement le système d'opposition des cartes Vitale reposait sur une liste, dite **liste d'opposition électronique** (LOE), diffusée mensuellement aux officines et aux serveurs de télé services. Elle permettait d'empêcher l'utilisation des cartes Vitale :

- devenues opposables au cours des six derniers mois ;
- ainsi que celle des cartes plus anciennement passées en opposition, sorties de la LOE, mais ayant de nouveau été utilisées en facturation dans l'année qui précède (ces cartes sont dites "réinjectées"»).

Depuis mars 2015, le système repose sur deux volets : l'un reposant sur les professionnels de santé et l'autre sur les régimes d'assurance maladie obligatoire (AMO).

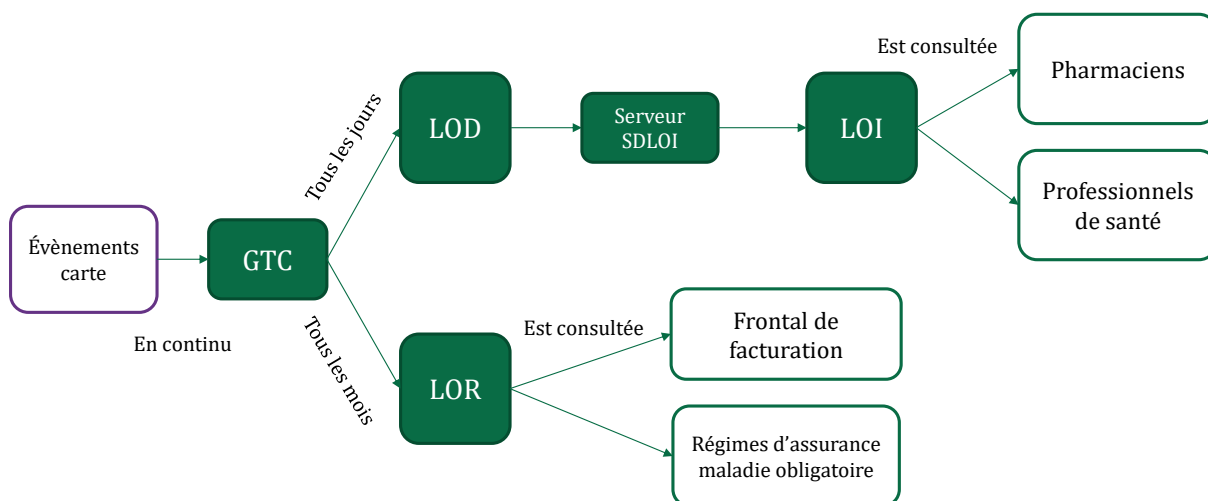
La GTC produit ainsi **trois listes d'oppositions** (cf. Graphique 5) :

- ◆ la **liste d'opposition directe** (LOD), qui intègre chaque jour les références des cartes Vitale ayant fait l'objet d'un évènement de fin de vie depuis la précédente édition de LOD ;
 - il s'agit de la liste des cartes en fin de vie pour tous motifs (cf. tableau 8) qui ne sont pas détruites ou invalidées ;
 - 50,3 millions de cartes inscrites en LOD en 2021, dont 6,8 millions de cartes inscrites en LOD suite à l'émission d'une nouvelle carte pour l'assuré ;

Annexe I

- ◆ une **liste d'opposition incrémentale (LOI)** :
 - il s'agit d'une **liste exhaustive des cartes en opposition mise à jour quotidiennement** par la GTC à partir des informations issues de la LOD ;
 - cette liste est utilisée par les **officines**, tenues depuis 2009 de mettre à jour à la liste quotidiennement⁵¹, et par les **professionnels de santé** ;
 - **diffusée par compléments successifs aux professionnels de santé** : seul le complément nécessaire est transmis. Il **ajoute les nouvelles cartes opposables et retire les cartes détruites ou invalidées** depuis la LOI précédente. Toutes les cartes deviennent opposables le lendemain de leur mise en fin de vie même si elles n'ont pas encore été utilisées en facturation ;
- ◆ une **liste d'opposition remontante (LOR)** :
 - diffusée **mensuellement** aux régimes d'assurance maladie obligatoire pour marquer l'opposition sur les cartes frauduleuses et abusives et envoyée aux professionnels de santé, aux AMO et au frontal de facturation pour permettre le contrôle de l'opposition ;
 - cette liste contient **toutes les cartes passées en opposition depuis l'origine, qui n'ont jamais été invalidées en mise à jour, ni détruites** ;
 - les **contrôles de liste d'opposition** sont faits dans les centraux des assurances maladie lors du traitement des FSE avec signalement déclenchant **contrôle systématique et processus de récupération de la carte Vitale**, en cas de paiement vers l'assuré pour un flux hors tiers payant, et avec un signalement au professionnel de santé pour un flux en tiers payant avec garantie de paiement accordée selon les accords conventionnels.
 - 2,13 millions de cartes inscrites en 2021 sur la LOR, dont 267 956 cartes entrées en LOR car ayant effectué indûment une FSE en 2021 ;
 - En 2021, 0,53 % des cartes en opposition avaient été utilisées pour établir une feuille de soins électronique (soit 15 081 cartes), contre 0,44 % en 2020 et 0,50% en 2019.

Graphique 5 : Constitution des listes d'opposition



Source : GIE SESAM-Vitale, mission.

⁵¹L'addendum numéro 4 au cahier des charges de la convention nationale des pharmaciens⁵¹, publié en mars 2009 prévoit que la LOI doit être téléchargée chaque jour.

Dans le système actuel, les cartes Vitale ayant servi à élaborer au moins une facture électronique après leur mise en fin de vie sont placées en liste d'opposition. Seules les cartes mises en fin de vie sous le motif « perdue/volée », « en incident » et « présumée abusive » sont mises en opposition directement. La mise en opposition directe des cartes Vitale modifie les modalités d'alimentation de la liste d'opposition incrémentale.

Le nombre de cartes en fin de vie dans la LOD a augmenté de 2,2 millions, soit une progression de 4,6% en 2021. Cette augmentation est notamment liée aux opérations de nettoyage du parc de cartes (cf. annexe II).

Pour la CPAM du Rhône, interrogée par la mission, en 2022, 8 516 flux ont été ciblés par un rejet ou un signalement en relation avec une anomalie liée à la carte vitale pour un montant de 350 752,69€. Ce montant rapporté aux montants versés à novembre 2022, de 2 132 515 638€ (soins de villes hors indemnités journalières), représente un **taux de 0,016% d'incidence financière.**

3. Si l'usage de la carte Vitale s'est généralisé pour les soins de ville, les téléservices de consultation des droits réduisent son apport et expliquent sa faible utilisation dans les établissements de santé

3.1. En complément de la carte Vitale, le développement du téléservice ADRI permet aux professionnels de santé libéraux de consulter les droits à jour des assurés

3.1.1. Le téléservice ADRI, actualisé quotidiennement, permet de parer à l'absence de mise à jour automatique des droits inscrits sur la carte Vitale

Par ailleurs, depuis 2015, la CNAM a développé le téléservice ADRI (Acquisition des DRoits Intégrée) à destination des professionnels de santé.

Ce téléservice **permet, en temps réel, de consulter les droits d'un assuré social, quel que soit son régime d'appartenance** et d'éviter ainsi d'établir une facturation fondée sur des informations qui ne sont pas à jour. Ce téléservice est intégré au sein des solutions logicielles des professionnels de santé, qui peuvent consulter, sur la base du NIR du patient, l'étendue de ses droits. Le téléservice ADRI permet aussi d'éviter les rejets de paiement lié aux écarts entre les droits de la Carte Vitale et les droits de la base de l'Assurance Maladie. De plus, les données récupérées sont automatiquement utilisées pour compléter la FSE, ce qui permet un gain de temps pour le professionnel de santé.

Les **données disponibles sur ADRI** sont les suivantes :

- ◆ **les droits du patient**, (C2S, ALD, droit de maternité, ACS, invalidité, et même, s'agissant de personnes n'ayant pas la qualité d'assuré social et ne détenant pas de carte Vitale, droits AME) auprès de l'Assurance Maladie Obligatoire (AMO), mais aussi auprès de l'Assurance Maladie Complémentaire (AMC), si celle-ci a été renseignée dans les bases de l'Assurance Maladie ;
- ◆ **le médecin traitant** ;
- ◆ l'organisme d'affiliation d'assurance maladie ;
- ◆ les **coordonnées** du patient ;
- ◆ la **validité de la carte Vitale** : si cette dernière a été déclarée comme perdue ou volée, au moment de la lecture avec le système ADRI, les droits du patient ne seront pas communiqués.

Annexe I

Le déploiement du recours à ADRI pour établir les feuilles de soins électroniques (FSE) a été rapide depuis 2015, traduisant l'intérêt de son utilisation pour les professionnels de santé libéraux. Les **appels au téléservice s'élevaient en 2022 à plus de 743 millions d'appels sur les onze premiers mois de l'année, soit dix fois plus qu'en 2018** (71,3 millions d'appels), et près de **deux fois plus qu'en 2020** (415,4 millions d'appels, cf. tableau 9).

Tableau 9 : Recours à ADRI pour l'établissement de feuilles de soins électroniques entre 2015 et 2022 (en millions)

Année	2015	2016	2017	2018	2019	2020	2021	2022 (11 mois)
Nombre de FSE	1315,1	1360,4	1371,1	1392,5	1414,5	1403,4	1624,4	1525,1
Nombre d'appels à ADRI	0,06	3,3	20,8	71,3	213,2	415,4	584,1	743,7

Source : GIE SESAM-Vitale, mission.

Pour les professionnels libéraux, la consultation d'ADRI peut être paramétrée dans le logiciel de cabinet :

- ◆ elle peut être **systématique**, par exemple quand le patient n'est pas connu du praticien ;
- ◆ elle peut être **effectuée au cas par cas**, le plus souvent lorsque l'assuré ne présente pas de carte Vitale mais une attestation de droits, voire ne présente aucun document.

Deux difficultés viennent toutefois entraver le bon fonctionnement de ce service :

- ◆ **le service est parfois indisponible**. En octobre 2022, 3,5% des requêtes avaient échoué sans que soit identifiée d'anomalie expliquant l'échec – par exemple l'assuré n'existe pas en base (ce taux dépassant 90% s'agissant des anciens ressortissants du RSI) ;
- ◆ **l'exhaustivité des données transmises est parfois défailtante**, ce qui pose notamment problème aux pharmaciens ;
 - à titre d'illustration, à l'occasion de la réunion de la commission paritaire locale de Saône et Loire du 24 mars 2022, la section professionnelle des pharmaciens relève « qu'ADRI ne permet pas de gérer deux exonérations », générant ainsi des rejets ;
 - dans le même cadre mais dans la Côte d'Or, un membre la section professionnelle indiquait, lors de sa réunion du 17 octobre 2022, que « lorsque l'assuré est en invalidité et en ALD, ADRI ne gère que l'ALD. Pour les soins hors ALD, le pharmacien facture alors avec application du ticket modérateur. Or, la facture est rejetée car elle aurait dû être facturée à 100% au titre de l'invalidité ». Le relevé de décision indique qu'une « nouvelle remontée sera faite à la CNAM ».

Par ailleurs, **le système ne permet pas** :

- ◆ **de mettre à jour la carte Vitale du patient** (cette opération nécessite un lecteur de puce spécifique), qui doit donc toujours se rendre dans une pharmacie, une caisse de l'Assurance maladie ou dans un établissement de santé ;
- ◆ **de bénéficier de la garantie de paiement** lors d'une consultation des droits effectuée sans que la carte Vitale du patient soit utilisée pour la signature de la FSE.

3.1.2. Amelipro offre également aux professionnels de santé un accès sécurisé aux informations relatives à leurs patients, à partir du NIR des assurés

Développé par la CNAM, l'espace numérique « Amelipro » accueille l'ensemble des téléservices accessibles aux professionnels de santé et connaît un développement important depuis plusieurs années. **En 2021, le nombre de sollicitations pour Amelipro a progressé de 43,8 % par rapport à 2020, s'établissant à 28,9 millions de connexions.**

Annexe I

Les données des patients concernant le rattachement et leurs droits sont accessibles **via leur Carte Vitale** ou en **saisissant uniquement leur NIR**.

Des services d'aide au suivi de l'activité, accessibles **sans carte CPS**, permettent, entre autres, au professionnel de santé de :

- ◆ consulter les paiements effectués par l'Assurance Maladie ;
- ◆ consulter les droits de base à l'Assurance Maladie des patients ;
- ◆ suivre les **indicateurs de la rémunération sur objectifs de santé publique (ROSP)**, de réaliser des déclarations et de consulter le détail des rémunérations ;
- ◆ consulter la liste des patients dont il est désigné médecin traitant et de visualiser les entrées et sorties de patientèle.

Des téléprocédures sécurisées avec la carte CPS facilitent la prise en charge des patients, y compris la création et la signature de FSE lors de visites⁵². Elles permettent, notamment :

- ◆ de consulter **l'historique de remboursement des soins médicaux** afin de bénéficier d'une meilleure connaissance du contexte médical des patients ;
- ◆ de consulter, créer, gérer ou suivre le renouvellement des protocoles de soins et d'effectuer une demande de mise en affectation de longue durée ;
- ◆ de réaliser une déclaration de grossesse ;
- ◆ de réaliser une déclaration de médecin traitant ;
- ◆ de créer, consulter et gérer une **prescription médicale de transport** en ligne.

Le professionnel de santé peut également **accéder aux téléservices depuis son logiciel métier**, et bénéficier au travers de cette interface de la grande majorité des services Amelipro, que ce soit en matière de prescription, de suivi des patients ou de déclaration de pathologies lourdes : prescription d'arrêt de travail, protocole de soins et ALD, déclaration de médecin traitant.

3.2. En établissement de santé, la consultation des droits est opérée au moyen des services en ligne de consultation des droits (CDR et CDRI) lors de la phase de pré-admission

S'agissant des établissements de santé, le processus de facturation se fait selon deux modalités principales :

- ◆ admission en soins urgents ;
- ◆ admission en soins programmés.

Les établissements de santé développent des procédures de pré-admission en ligne pour les patients dont les soins sont programmés, dans le but de simplifier les formalités de l'admission et de fluidifier le parcours des patients⁵³. Lors de cette phase de préadmission, la consultation des informations personnelles du patient et des droits au titre de l'assurance maladie obligatoire, est opérée au moyen des services en ligne de consultation des droits (CDR et CDRI) :

- ◆ l'outil CDRI est intégré au logiciel métier de l'établissement de santé ;
- ◆ l'outil CDR est accessible au moyen d'une connexion spécifique, et nécessite, une fois les informations consultées, de les saisir dans le logiciel métier (cf. tableau 10).

⁵² Au moyen d'un « terminal lecteur applicatif (TLA) complet.

⁵³ Elles prévoient notamment la transmission d'une copie scannée d'une pièce d'identité et de la carte Vitale : la puce de la carte Vitale n'est pas consultée, seul le NIR affiché sur la carte est exploité (voire la photographie).

Annexe I

Il n'est toutefois pas possible de connaître les droits ouverts au titre de l'assurance maladie complémentaire par le biais de ces téléservices⁵⁴.

Tableau 10 : Comparaison des outils de consultation des droits : CDRI et CDR

Service	Usage	Modalités d'accès	Informations obtenues
CDRI	Récupération automatisée des droits des assurés et intégration dans la facture.	Le service nécessite une carte CPE nominative, CDE, CPS ou CPF. L'appel du service s'effectue avec le NIR de l'ouvrant droit, et la date et le rang de naissance du patient. Ces informations sont obtenues à partir de la consultation par le logiciel de la carte Vitale du patient ou de la base Patient. Elles peuvent être saisies à partir d'une autre source d'informations (service CDR, attestation de droits).	Identification du patient (nom, prénom, date de naissance, NIR de l'assuré) ; droits de base ; exonérations ; AME de base ; couverture maladie, AT/MP, maternité ; C2S ; ACS ; identification du médecin traitant ; adresse de l'ouvrant droit
CDR	Récupération manuelle des droits des assurés nécessitant une ressaisie dans le logiciel de gestion administrative patient.	Le service nécessite une carte CPE nominative, CDE, CPS ou CPF. La recherche s'effectue en saisissant le NIR de l'ouvrant droit ou, à défaut, les nom/prénom et date de naissance du patient. Ces informations sont obtenues à partir de la base Patient ou d'un autre support (carte Vitale, attestation de droits).	Identification du patient (nom, prénom, date de naissance, NIR de l'assuré) ; droits de base ; Exonérations ; AME de base ; couverture maladie ; CMU-C ; ACS ; identification du médecin traitant (nom, prénom, n° AM)

Source : CNAM.

⁵⁴ À l'instar de la carte Vitale, dont les droits en puce ne comprennent que ceux ouverts au titre de l'assurance maladie obligatoire.

3.2.1. Dans le cadre de soins urgents en établissement de santé, il est fréquent de ne pas présenter de carte Vitale

Depuis le 1^{er} janvier 2022, une tarification particulière, le « **forfait patient urgences (FPU)** »⁵⁵ d'un montant de 19,61 €, s'applique à chaque personne qui se rend aux urgences pour des soins non programmés et qui sort des urgences sans être hospitalisée. Selon la situation des patients, le FPU est minoré à 8,49 €⁵⁶, voire supprimé⁵⁷.

L'établissement adresse par ailleurs à l'organisme d'assurance maladie obligatoire du bénéficiaire des soins, une **facture comportant le report de ce FPU, ainsi que d'autres forfaits tenant compte du profil du patient et des soins dispensés** (complément du FPU, forfait activité socle en fonction de l'âge du patient, éventuels suppléments forfaitaires).

Dans le cadre d'un passage au service des urgences, **le patient est soigné sans que la présentation de la carte Vitale ne soit un préalable**. L'instruction administrative se fait après l'examen aux urgences (ou parallèlement, si le patient est accompagné d'un tiers) afin de déterminer la situation du patient au regard du FPU et de la facturation des soins.

S'il s'avère que le patient ne bénéficie pas de droits ouverts à l'assurance maladie ni de l'aide médicale d'État, les frais liés aux soins urgents sont à la charge du patient. Néanmoins, lors d'échanges avec divers hôpitaux publics⁵⁸, la mission a pu constater que les difficultés rencontrées par les établissements de santé pour obtenir le paiement des factures émises à la suite d'un passage aux urgences les conduisent régulièrement à renoncer à leurs créances auprès des patients qui sont fréquemment insolvables. En 2021, l'abandon de créances liées à des hospitalisations non réglées par les patients, a conduit l'hôpital universitaire Avicenne à inscrire plus de 2,6 M€ en admissions en non-valeur⁵⁹ (4,6 M€ en 2020).

3.2.2. Lors de l'admission dans le cadre de soins programmés, la carte Vitale n'est employée que pour obtenir le NIR des patients afin de consulter CDR ou CDRi afin de vérifier l'existence et la nature des droits sociaux ouverts

Lors d'une admission en soins programmés, trois étapes principales se succèdent :

- ◆ **le patient doit, préalablement aux soins, remplir des formalités administratives** (bureau des admissions) :
 - à cette occasion, **il est demandé de présenter la carte Vitale ou tout document utile à l'établissement pour établir l'existence de droits** lui permettant de facturer les soins à l'assurance maladie (lorsque le patient est assuré social) ou à l'État (lorsque le patient ressort de l'aide médicale d'État).

⁵⁵ L.162-22-11-1 du code de la sécurité sociale

⁵⁶ Personnes en affection de longue durée (ALD) ; personnes qui bénéficient de prestations suite à un accident du travail ou une maladie professionnelle avec une incapacité inférieure à deux tiers.

⁵⁷ Femmes enceintes bénéficiaires de l'assurance maternité ; bénéficiaires d'une pension d'invalidité ; bénéficiaires de prestations suite à un accident du travail ou une maladie professionnelle ayant une incapacité supérieure à deux tiers assurés mineurs victimes de violences sexuelles ; nouveau-nés de moins d'un mois ; donneurs d'organe ; titulaires d'une pension militaire d'invalidité ; victimes d'actes de terrorisme ; bénéficiaires de l'aide médicale d'État (AME) ; personnes écrouées.

⁵⁸ Hôpital universitaire Avicenne, AP-HP ; centre hospitalier de Perpignan, conférence des DG de CHU, notamment.

⁵⁹ Titres admis en non-valeur par le comptable (TANV).

Annexe I

- divers autres documents, comme les droits à l'assurance maladie complémentaire ou un document d'identité⁶⁰ peuvent lui être demandés à cette occasion. Cette phase peut être effectuée très **en amont de l'hospitalisation elle-même**, des jours voire des semaines avant celle-ci ;
 - à titre d'illustration, sur les 43 admissions de patients effectuées lors de la semaine du 6 février 2023 à l'hôpital Avicenne (AP-HP), 23 admissions ont été faites en l'absence de carte Vitale du patient. Des documents d'identité (carte nationale d'identité ou autre titre) ont quant à eux été présentés lors de 42 des 43 admissions ;
 - **l'existence de droits est établie à partir du NIR du patient**, à partir duquel sont consultés les droits ouverts sur le logiciel métier de l'établissement (CDRi) ou en consultant directement le téléservice CDR ;
- ◆ les **soins sont prodigués** par l'équipe soignante de l'établissement ;
 - ◆ sur la base du dossier patient, les soins apportés sont ensuite codés⁶¹, classés dans une grille décrivant la maladie et reprenant la nomenclature établie lors de la 10^{ème} révision de la classification internationale des maladies de l'OMS (2018) puis présentés au **paiement de l'organisme d'assurance maladie** dont relève le patient pour les établissements dits ex-OQN (pour l'essentiel, les structures à but lucratif), et présentés à la facturation de l'assurance maladie après un processus administratif complexe pour les établissements dits ex-DG (pour l'essentiel les autres structures).

Contrairement à la situation prévalant dans les petites structures de soins de ville, les phases d'identification du patient et de ses droits, de soins, et enfin de facturation aux organismes d'assurance maladie sont réalisées par des personnes différentes et nécessitent la mise en place d'une organisation coordonnée entre ces multiples acteurs, l'échelon administratif intervenant aux deux extrémités de la chaîne.

Les établissements de santé développent des **solutions logicielles de préadmission** afin de permettre au patient d'apporter les éléments à son rythme depuis son domicile, ce qui permet à l'établissement de réduire les tensions sur le service des admissions et de fluidifier les flux ;

Par ailleurs, le **tiers payant est la règle pour la part couverte par l'assurance maladie obligatoire**⁶² (CSS, art. L. 162-21-1), ce qui nécessite une attention particulière à l'existence de droits pour les patients. Ainsi, **deux consultations** peuvent être effectuées :

- ◆ une première consultation lors de la phase d'admission, le défaut de droits bloquant le processus ;
- ◆ une deuxième consultation, lors de l'entrée en hospitalisation, afin de s'assurer avant les soins que les droits sont bien ouverts à la date des soins.

Lors de sa visite à l'hôpital Avicenne en janvier 2023, la mission a pu constater que **les équipes en charge de l'admission ne faisaient pas usage du lecteur de carte vitale**. La consultation de CDR et de CDRi (consultation des droits intégrée⁶³) s'y substituait afin de disposer de la situation des droits à jour.

⁶⁰ Code de la sécurité sociale, art. L. 161-21.

⁶¹ Annexée, pour sa dernière version, à l'arrêté du 28 mars 2022 (JORF du 8 avril 2022), et reprenant un numéro (GHS – groupe homogène de soins) et un code (GHM – groupe homogène de malades).

⁶² Ces dispositions ne s'appliquent pas à l'assurance maladie complémentaire dans les cas où la couverture par l'assurance maladie obligatoire n'est pas intégrale. Voir la participation financière des patients à l'hôpital : analyse des conditions pour la mise en œuvre d'une réforme du ticket modérateur, IGAS [2014-164R]-IGF [2014-M-085-03], mai 2015.

⁶³ Il existe également un téléservice CDR, qui donne des informations presque identiques, avec une consultation manuelle et non automatique comme dans CDRi. Contrairement à CDRi qui nécessite le NIR ou des informations équivalentes, la consultation peut s'effectuer sur la base des seuls noms, prénoms et date de naissance du patient.

Annexe I

En 2022, le GIE SESAM-Vitale fait état de 70 millions d'appels CDRi (intégrés aux logiciels de gestion des établissements de santé) et de 316 millions de consultations à CDR, téléservice accessible en ligne et qui n'est pas intégré au logiciel de facturation. 188 millions de factures B2 ont été établies par 3 600 établissements connectés aux téléservices.

Tableau 11 : Recours à CDRi pour l'établissement de feuilles de soins électroniques entre 2015 et 2022, France entière (en millions)

Année	2015	2016	2017	2018	2019	2020	2021	2022 (11 mois)
Nombre de FSE	1315,1	1360,4	1371,1	1392,5	1414,5	1403,4	1624,4	1525,1
Nombre d'appels à CDRi	-	0,08	1,7	17	35,5	46,7	61,1	71,4

Source : GIE SESAM-Vitale, mission.

ANNEXE II

**Les cartes Vitale surnuméraires et les
résidents affiliés à l'assurance maladie**

SOMMAIRE

1. LA PROBLÉMATIQUE DES CARTES SURNUMÉRAIRES EST DÉSORMAIS BIEN EXPLORÉE ET LE RISQUE D'UNE UTILISATION FRAUDULEUSE MASSIVE EST DORÉNAVANT MAÎTRISÉ.....	1
1.1. Les modalités de délivrance des cartes Vitale et de gestion du parc ont conduit à des divergences entre le nombre d'assurés et le nombre de cartes Vitale valides.....	1
1.1.1. <i>La détention de la carte Vitale n'étant pas obligatoire, certains assurés éligibles n'en disposent pas, notamment les mineurs, sans que leur nombre soit connu</i>	<i>2</i>
1.1.2. <i>Le stock de cartes surnuméraires a atteint plusieurs millions d'unités.....</i>	<i>2</i>
1.2. L'assurance maladie a mis en place des mesures qui ont conduit à résorber le stock de cartes surnuméraires	3
1.2.1. <i>L'assurance maladie a mis en place des mesures pour maîtriser son parc de cartes Vitale lors de l'émission</i>	<i>4</i>
1.2.2. <i>Depuis 2016, plus de trois millions de cartes ont été mises en fin de vie dans le cadre d'opérations d'épuration des bases.....</i>	<i>5</i>
1.2.3. <i>Les opérations de fiabilisation du parc de cartes Vitale a conduit à la très forte résorption du nombre de cartes Vitale surnuméraires</i>	<i>6</i>
1.3. Le risque de facturation sans droits au moyen de cartes Vitale invalides est limité protégeant ainsi les régimes d'assurance maladie d'éventuels préjudices financiers en cas d'utilisation de cartes surnuméraires	9
2. DES LIMITES MÉTHODOLOGIQUES STRUCTURELLES CONDUISENT À UN ÉCART PEU INTELLIGIBLE ENTRE LE NOMBRE DE RESSORTISSANTS DES RÉGIMES D'ASSURANCE MALADIE ET LA POPULATION LÉGALE, QUI NE SE CORRESPONDENT PAS	11
2.1. La population française est connue par le recensement, mais l'INSEE gère aussi le RNIPP, qui rassemble les identités des personnes nées en France ou y ayant résidé.....	11
2.1.1. <i>La population légale est établie sur la base d'une enquête statistique, le recensement.....</i>	<i>12</i>
2.1.2. <i>Le répertoire national d'identification des personnes physiques (RNIPP) contient aussi des informations sur la population.....</i>	<i>13</i>
2.1.3. <i>Les deux outils ne sont pas rapprochés ce qui peut occasionner des difficultés</i>	<i>14</i>
2.2. La population assurée française est connue de manière incrémentale sur la base de données administrative.....	15
2.3. Certaines personnes résidant en France ne sont pas assurées sociales	16
2.3.1. <i>Certains travailleurs détachés entrants peuvent relever de régimes de sécurité sociale étrangers.....</i>	<i>16</i>
2.3.2. <i>Les travailleurs frontaliers communautaires sortants ne relèvent généralement pas de la sécurité sociale française.....</i>	<i>17</i>
2.3.3. <i>Certains travailleurs frontaliers avec la Suisse y sont affiliés pour le risque maladie.....</i>	<i>17</i>
2.3.4. <i>Les étudiants étrangers du programme ERASMUS demeurent en principe affiliés à leur régime d'origine.....</i>	<i>18</i>

2.3.5.	<i>Certains territoires français non couverts par l'assurance maladie permettent la couverture de leurs ressortissants par cette dernière.....</i>	18
2.4.	<i>Inversement, certains assurés sociaux peuvent ne pas résider en France</i>	18
2.4.1.	<i>Les travailleurs détachés sortants demeurent en principe affiliés en France</i>	19
2.4.2.	<i>Les titulaires d'une pension de vieillesse, d'invalidité ou d'inaptitude française et résidant à l'étranger bénéficient de la prise en charge de leurs frais de santé.....</i>	19
2.4.3.	<i>Les étudiants étrangers étudiant en France relèvent de la sécurité sociale française sans nécessairement être résidents français.....</i>	20
2.4.4.	<i>Les étudiants français du programme ERASMUS étudiant à l'étranger relèvent de la sécurité sociale française sans nécessairement être résidents en France</i>	20
2.4.5.	<i>Les travailleurs saisonniers ne sont pas résidents français mais ont des droits à l'assurance maladie française.....</i>	21
2.4.6.	<i>En fonction des conventions bilatérales, les résidents de certains pays peuvent voir pris en charge leurs frais de santé par la sécurité sociale française.....</i>	21
2.5.	<i>Un écart entre la population assurée et la population résidente demeure.....</i>	22

L'écart entre la population résidant en France et le nombre de cartes vitales actives en circulation a suscité de nombreux questionnements en 2020 lors des auditions de la Commission d'enquête de l'Assemblée nationale relative à la lutte contre les fraudes aux prestations sociales.

Par ailleurs¹, « *la mission confiée par le Premier ministre à Mme Nathalie Goulet et à Mme Carole Grandjean avait [...] soulevé ce point sensible, en calculant qu'il y avait **environ 5,25 millions de cartes Vitale « actives » en surnombre par rapport au nombre de porteurs potentiels**. Ce concept de carte « active » désigne une carte sur laquelle des droits à remboursement par l'assurance maladie sont ouverts et qui n'a pas été désactivée ou mise en opposition. Ce chiffre était calculé comme l'écart entre le nombre de cartes actives en circulation (59,4 millions) et le nombre de bénéficiaires potentiels (54,15 millions de personnes de plus de 16 ans). Ce nombre de cartes en surnombre descendait à 1,92 million si le nombre de cartes en circulation était comparé à l'ensemble de la population de plus de douze ans (57,48 millions), âge à partir duquel les parents peuvent faire une demande de carte Vitale pour leur enfant* ».

La Cour des comptes recommandait dans son rapport sur la lutte contre la fraude sociale (septembre 2020), « **d'éteindre l'excédent de cartes valides (un peu moins de 153 000 fin juin 2020) par rapport au nombre d'assurés ayant des droits ouverts à l'assurance maladie, la détention de plusieurs cartes par un même ou au nom d'un même assuré suscitant un risque particulier de remise à un tiers.** »

Les débats portent ainsi sur deux objets différents :

- ◆ l'écart entre le nombre de cartes Vitale actives en circulation et celui de la population affiliée à l'assurance maladie;
- ◆ l'écart entre la population affiliée à l'assurance maladie et la population recensée par l'INSEE.

1. La problématique des cartes surnuméraires est désormais bien explorée et le risque d'une utilisation frauduleuse massive est dorénavant maîtrisé

Pour des raisons historiques, un stock de cartes surnuméraires s'est constitué (1.1). Toutefois, depuis 2010 et avec une accélération notable, ce stock a été progressivement résorbé (1.2). Au surplus, le risque financier lié au mésusage des cartes surnuméraires apparaît maîtrisé (1.3).

1.1. Les modalités de délivrance des cartes Vitale et de gestion du parc ont conduit à des divergences entre le nombre d'assurés et le nombre de cartes Vitale valides

La détention de carte Vitale n'étant pas obligatoire, leur nombre devrait être inférieur à celui des assurés sociaux (1.1.1). Pourtant, pour des raisons historiques, un stock de cartes Vitales surnuméraires s'est constitué (1.1.2).

¹ Rapport fait au nom de la commission d'enquête relative à la lutte contre la fraude aux prestations sociales, M. HETZEL (président) et M. BRINDEAU (rapporteur), Assemblée nationale, 8 septembre 2020.

1.1.1. La détention de la carte Vitale n'étant pas obligatoire, certains assurés éligibles n'en disposent pas, notamment les mineurs, sans que leur nombre soit connu

La détention d'une carte Vitale ne constitue pas une obligation. Il n'y a donc pas de lien automatique entre l'affiliation et la production d'une carte Vitale. Il est possible de faire valoir ses droits à l'assurance maladie en produisant par exemple une attestation papier

Toute personne affiliée à la sécurité sociale a la **faculté de demander l'établissement d'une carte Vitale personnelle dès 12 ans**. La délivrance est à l'initiative de l'assuré social et de ses représentants légaux. L'Assurance maladie propose à tous ses ressortissants l'attribution d'une carte Vitale à partir de l'âge de 16 ans.

Interrogée par la mission, le GIE SESAM-Vitale n'a pas été en mesure d'estimer le nombre d'assurés sociaux ayant déjà été destinataires d'une carte Vitale.

Par ailleurs les **délais de production de la carte Vitale génèrent un sous-équipement « frictionnel » des assurés**. Si les délais moyens de production s'établissent à dix jours (cf. annexe I), ces délais ne tiennent pas compte des démarches préalables de l'assuré, notamment la transmission d'une photographie dans un format valide, et d'éventuelles difficultés d'instruction pouvant durer plusieurs mois entre la demande initiale et la délivrance de la carte.

1.1.2. Le stock de cartes surnuméraires a atteint plusieurs millions d'unités

Dans la situation qui prévalait avant 2010, aucun système n'inscrivait les cartes surnuméraires issues d'une perte (et parfois retrouvées et réutilisées par leur porteur légitime) ou d'un changement de régime en liste d'opposition : valides, elles ne pouvaient toutefois pas être utilisées, lorsque le régime rejetait le remboursement d'un assuré qui n'y avait plus de droits, et en toute hypothèse une fois leur date de validité dépassée. N'étant pas inscrites en liste d'opposition, elles n'étaient pas invalidées, accroissant ainsi un stock de cartes Vitale non invalidées. Surtout, avant 2010, un changement de régime entraînait automatiquement l'émission d'une nouvelle carte Vitale sans que la carte précédente ne soit systématiquement invalidée.

Ainsi, les différents régimes d'assurance maladie ont accumulé au fil des ans des excédents de cartes, pour atteindre **un montant cumulé de 2,35 millions de cartes excédentaires en 2018²**.

Par commodité de raisonnement, la comparaison est effectuée entre :

- ◆ d'une part le **nombre de cartes Vitale actives émises par un régime** ;
- ◆ et d'autre part le **nombre d'assurés sociaux relevant de ce régime**.

Le nombre de cartes surnuméraires est la différence entre le premier et le second chiffre lorsqu'elle est positive. Il s'agit là d'une **définition « collective »** de la notion de carte surnuméraire, la collectivité étant le régime d'assurance maladie (on dénombre les cartes surnuméraires pour chaque régime).

Pour autant, ce raisonnement est imparfait puisque **des assurés peuvent ne pas être équipés de carte Vitale et compenser ainsi tout ou partie de carte Vitale multiples attribués à d'autres assurés**. La définition « individuelle » de la notion de carte surnuméraire est apparue inopérante à la mission en l'absence de données permettant de vérifier cet équilibre au sein de chaque régime.

² Près de 8 millions en 2012 d'après le rapport IGAS [RM2013-146P] / IGF [2013-M-014-02] sur les coûts de gestion de l'assurance maladie, septembre 2013.

Annexe II

Ainsi, le terme « **carte Vitale surnuméraire** » sera utilisé afin de désigner l'ensemble des cartes Vitale dépassant le nombre de personnes affiliées à un régime, qui est la convention couramment retenue. Cela ne signifie pas que, ponctuellement, aucun assuré social ne dispose de plusieurs cartes Vitale valides.

Fin 2021, le parc de cartes Vitale était composé de 57,9 millions de cartes valides alors que 60,1 millions d'assurés auraient pu détenir une carte Vitale (cf. graphique 2).

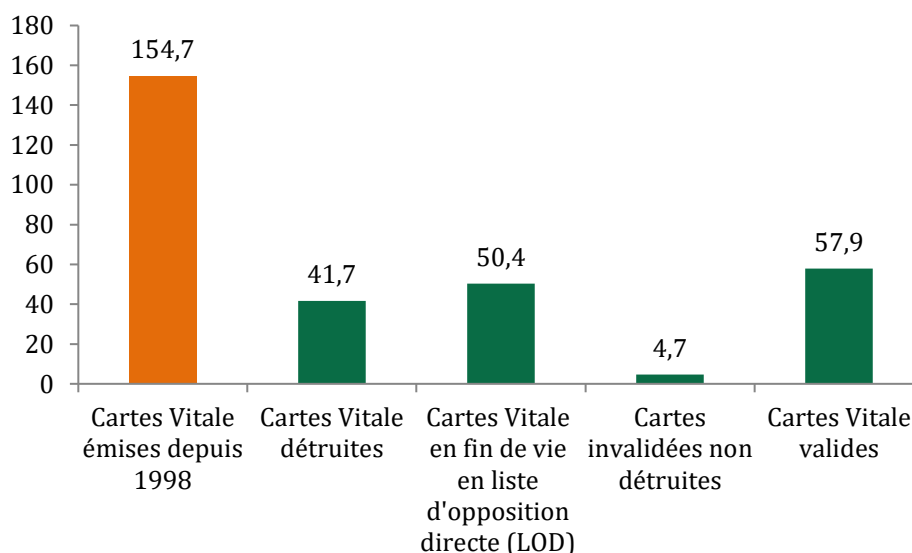
Au 31 décembre 2021, 154,7 millions de cartes Vitale avaient été émises depuis 1998, dont 57 millions de cartes Vitale 2. Au sein de ce parc total, 41,7 millions de cartes avaient déjà été détruites et 4,7 millions de cartes avaient été invalidées mais pas détruites. (cf. annexe I).

Tableau 1 : Statut du parc de cartes Vitale émises depuis 1998, au 31 décembre 2021

Statut	Parc Global	Vitale 1	Vitale 2
Cartes émises depuis 1998	154,7	97,7	57,1
Cartes détruites	41,7	34,8	6,9
Cartes invalidées non détruites	4,7	2,9	1,8
Cartes en fin de vie en LOD	50,4	38,7	11,7
Cartes valides	57,9	21,2	36,7

Source : GIE-SESAM-Vitale.

Graphique 1 : Composition du parc de cartes Vitale émises depuis 1998, au 31 décembre 2021



Source : GIE SESAM-Vitale.

1.2. L'assurance maladie a mis en place des mesures qui ont conduit à résorber le stock de cartes surnuméraires

L'assurance maladie a mis en place des mesures afin de maîtriser son parc de cartes Vitale :

- ♦ en sécurisant le processus d'émission, notamment n'émettant plus de nouvelle carte Vitale lors d'un changement de régime (1.2.1) ;
- ♦ en procédant à des campagnes d'épuration des bases s'agissant des cartes détenues par des assurés décédés ou n'étant plus titulaires de droits (1.2.2).

Ces mesures ont conduit à la forte résorption du stock de cartes surnuméraires, qui ne demeurent que dans quelques régimes de manière marginale (1.2.3).

1.2.1. L'assurance maladie a mis en place des mesures pour maîtriser son parc de cartes Vitale lors de l'émission

Pour l'essentiel, le surnombre de cartes Vitale était une conséquence des règles mises en place lors du lancement de la carte en 1998 et des contraintes techniques initiales.

Afin de mieux maîtriser son parc de cartes Vitale, l'assurance maladie et le GIE SESAM-Vitale ont mis en place des mesures pour sécuriser le système d'émission des cartes et les facturations et plusieurs campagnes de croisement de données ont été menées afin d'invalider les cartes Vitale surnuméraires :

- ◆ **avant 2010**, il n'était pas possible pour un assuré de conserver sa carte Vitale lorsqu'il changeait de régime. Une nouvelle carte devait être éditée, sans restitution obligatoire de l'ancienne ;
- ◆ **la vérification de l'existence d'une carte Vitale déjà attribuée à un assuré a été mise en place en 2010**. Si une ancienne carte Vitale affectée à l'assuré existait, le régime était alerté ; il lui appartenait ensuite d'effectuer la mise en opposition ;
- ◆ **depuis 2019, la mise en opposition systématique, est effectuée** : lorsqu'une nouvelle carte Vitale est émise pour un assuré, le numéro de l'ancienne carte reste sauvegardé dans la base de gestion technique des cartes (GTC) et une mise en opposition automatique est réalisée.

Le GIE SESAM-Vitale ne dispose pas des informations permettant de faire le lien entre un assuré et une carte Vitale :

- ◆ la **base de données GTC** ne traite que des numéros de cartes et des événements de « vie » des cartes Vitale ;
- ◆ **c'est au sein du RNIAM³, sous la responsabilité de la CNAV, qu'est établi le lien entre assuré et numéro de série de la carte**. Les informations contenues dans le RNIAM sont confrontées à celles provenant respectivement du RNIPP, tenu par l'INSEE, et des organismes gérant les régimes de base d'assurance maladie. Le RNIAM contribue ainsi aux procédures de délivrance et de mise à jour des cartes Vitale.

Lors de la procédure, le régime gestionnaire de l'ancienne carte Vitale (connu dans la base de données GTC) et le régime gestionnaire précédent de la carte (connu dans la base de données GTC s'il y en avait un) sont respectivement informés de la mise en opposition de la carte.

S'agissant de l'émission de la carte Vitale, **depuis 2010** : un **portail inter-régimes** a été mis en place qui permet d'éviter l'émission d'une nouvelle carte si l'ancienne n'a pas été restituée ou invalidée. Ce processus de mutation permet de conserver la même carte Vitale en changeant de régime, une simple mise à jour (par exemple en pharmacie d'officine) permettant d'opérer le changement de régime en carte.

Il en résulte que des **cartes Vitale ont pu être délivrées « en doublon » avant 2010**. En effet, on peut faire l'hypothèse que les assurés sociaux déclarent à l'assurance maladie leurs cartes Vitale perdues et surtout volées dans un bref délai, notamment lorsqu'ils engagent les démarches pour la remplacer.

Depuis septembre 2019, les cartes détectées en doublon sont inscrites en liste d'opposition, notamment celles qui correspondaient à des mutations de régime antérieures à 2010.

³ Répertoire national inter-régimes des bénéficiaires de l'assurance maladie, contenant les données servant à l'immatriculation des assurés sociaux (NIR, nom et prénoms, date et lieu de naissance, information sur le décès ou la mention que la personne n'est plus bénéficiaire de l'assurance maladie, l'organisme d'assurance maladie de rattachement et éventuellement l'organisme complémentaire).

Un audit de la CNAM réalisé en 2022, a conduit à **identifier les cartes Vitales ayant un NIR identique et en gestion dans plusieurs caisses**. Un échantillon de 28,3 millions de cartes Vitale a été constitué à partir de cartes à la fois valides (état dans la base de gestion des cartes) et reconnues par un régime d'assurance maladie (état « en gestion »). L'analyse a permis d'identifier 3 722 NIR disposant de plusieurs cartes Vitale dans deux caisses, et 2 NIR disposant de deux cartes Vitale dans trois caisses. Cela représente **0,013 % des cartes Vitale de l'échantillon et correspond à un problème de doublons frictionnels**, issus de la non-finalisation du processus de mise à jour des systèmes d'information. La régularisation s'opère toutefois lorsque le processus de mise à jour est mené à son terme.

1.2.2. Depuis 2016, plus de trois millions de cartes ont été mises en fin de vie dans le cadre d'opérations d'épuration des bases

L'Assurance Maladie procède depuis 2016 à des opérations de mise en fin de vie des cartes Vitale (cf. graphique 2) dont les titulaires n'ont plus de droits ou dont les titulaires sont décédés ou radiés. Ces cartes mises en fin de vie dans le système sont placées automatiquement en **liste d'opposition**.

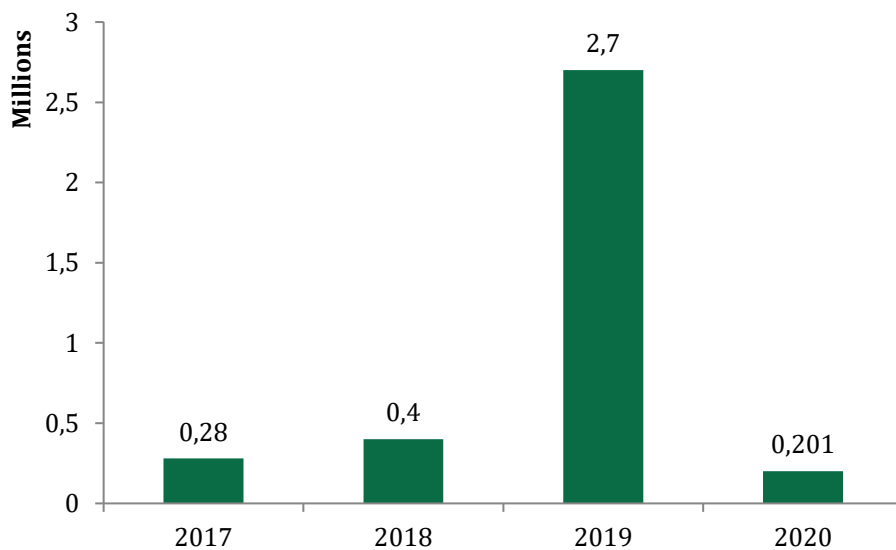
Pour le régime général, les opérations suivantes ont été effectuées **entre 2017 et 2020** :

- ◆ en 2017, 280 000 cartes Vitale appartenant à des **bénéficiaires n'ayant pu justifier de leurs droits** ont été placées en liste d'opposition (les droits du bénéficiaire étant clos, la facturation avec ces cartes Vitale n'était plus possible) ;
- ◆ en 2018, 400 000 cartes Vitale appartenant à des **porteurs décédés** ont été placées en liste d'opposition lors d'une campagne programmée (la mise en fin de vie, réalisée uniquement de manière manuelle, étant parfois oubliée au moment de la prise en compte du décès du porteur). Cette action a été complétée par une seconde opération de mise en fin de vie des **cartes non mutées pour des porteurs ayant changé de régime depuis plus de 27 mois** ;
- ◆ **2,7 millions de cartes Vitale non précédemment mises en fin de vie ont été placées en liste d'opposition** en 2019. Deux opérations ont été conduites:
 - en préalable au transfert de la population des travailleurs indépendants vers le régime général, le GIE SESAM-Vitale a comparé le parc de cartes vu du régime SSTI avec la situation en GTC (détection de 800 000 cartes valides à tort en GTC)⁴ ;
 - depuis septembre 2019, toutes les cartes détectées en doublon sont insérées en liste d'opposition. Cette opération a permis de reprendre les cartes qui n'ont pas été confirmées par les régimes depuis la mise en place du PEC en 2010 (800 000 cartes).
- ◆ en 2020, 201 000 **cartes Vitale délivrées suite à des anomalies du système d'information en cas de mutation des bénéficiaires ont été placées en liste d'opposition** (les droits du bénéficiaire étant clos dans la caisse cédante, la facturation n'est alors plus possible).

⁴ Cette opération a été complétée avec les parcs de cartes de la MSA et des mutuelles étudiantes régionales (mise en fin de vie de 340 000 cartes pour MSA et 500 000 pour les SMER) ;

Annexe II

Graphique 2 : Cartes mises en liste d'opposition par le régime général suite à des campagnes ciblées entre 2017 et 2020 (en millions)



Source : GIE SESAM Vitale.

1.2.3. Les opérations de fiabilisation du parc de cartes Vitale a conduit à la très forte résorption du nombre de cartes Vitale surnuméraires

Début 2019, le nombre de cartes surnuméraires s'établissait à plus de 2,5 millions (cf. tableau 2).

Annexe II

Tableau 2 : Comparaison entre le nombre de porteurs potentiels de cartes Vitale de plus de 16 ans⁵ et le nombre de carte Vitale par régime au 31 décembre 2018

Régime	Porteurs potentiels de plus de 16 ans-	Cartes Vitale valides	Cartes surnuméraires	Cartes valides/Porteurs potentiels
01- Régime Général	45 163 570	43 367 835	-	96%
02- Régime Agricole – MSA	2 790 220	3 141 869	351 649	113%
03- S.S.I.	3 872 483	4 479 689	607 206	116%
04- S.N.C.F	393 389	465 818	72 429	118%
05- R.A.T.P	85 836	101 752	15 916	119%
06- ENIM (Marine)	88 996	96 306	7 310	108%
07- Mines	107 339	162 431	55 092	151%
08- Militaires de Carrière	668 095	768 886	100 791	115%
10- Clercs, Employés de Notaire	94 626	119 505	24 879	126%
14- Assemblée Nationale	4 849	5 100	251	105%
15- Sénat	3 450	4 207	757	122%
90- C.A.V.I.M.A.C. (cultes)	42 209	97 529	55 320	231%
91- M.G.E.N	2 551 751	2 520 351	-	99%
92- Mutuelle des PTT ⁶	6 869	147 357	140 488	NS
93- Mutuelle Générale Police	124 432	184 333	59 901	148%
94- Fédération. Fonctionnaires (SLI ⁷)	821 833	840 395	18 562	102%
95- M.N.H.	248 894	294 264	45 370	118%
96- Harmonie Fonction Publique	162 161	167 893	5 732	104%
99- Autres Mutuelles	1 678 936	2 470 516	791 580	147%
Total	58 909 938	59 436 036	2 353 233	-
Dont hors CNAM	13 746 368	16 068 201	2 353 233	-

Source : CNAM

Au 31 décembre 2019, le nombre de cartes valides était déjà inférieur (de 400 000) au nombre de personnes affiliées, estimé au moyen du RNIAM. Cette évolution s'explique par de grandes opérations d'épuration du parc de cartes menées en 2019 :

- ◆ en préparation du transfert de la population des travailleurs indépendants vers le régime général, le GIE SESAM-Vitale a comparé le parc de cartes vu du régime des indépendants avec la situation en base de gestion technique des cartes. Cela a permis de détecter 800 000 cartes surnuméraires ;
- ◆ cette opération a été complétée avec les parcs de cartes de la MSA et des mutuelles étudiantes régionales :
 - mise en fin de vie de 340 000 cartes pour MSA ;
 - mise en fin de vie de 500 000 cartes pour les mutuelles étudiantes.

De nouvelles opérations d'épuration du parc de carte menées en 2020 ont permis de résorber le nombre de cartes surnuméraires dans de nombreux régimes (régime général, CAMIEG, CAVIMAC, ENIM, CRPCEN, RATP, SNCF, militaires, mutuelles de fonctionnaires...), entraînant la mise en fin de vie d'environ 1,5 million de cartes Vitale.

⁵Bénéficiaires de l'assurance maladie certifiés rattachés au RNIAM (Registre National Inter-Régimes des bénéficiaires de l'Assurance Maladie) non décédés, et âgés de 16 ans et plus.

⁶ Fin des délégations de gestion du régime obligatoire entre 2018 et 2020 pour les mutuelles de fonctionnaires de la fonction publique d'État, à l'exception de la MGEN.

⁷ Section locale interministérielle

Annexe II

Des traitements réguliers de mise en fin de vie par exemple des personnes décédées contribuent à cette gestion du parc (exemple de traitement passé sur les cartes des décédés en juin 2020 pour 11 000 cartes mises en fin de vie).

Ainsi, au 31 décembre 2020, le nombre total de cartes valides est inférieur de 2,3 millions au nombre de porteurs théorique, estimés à partir du RNIAM.

Les dernières statistiques datant de septembre 2022 font état de 949 cartes surnuméraires pour l'ensemble des régimes (cf. tableau 3). Elles se répartissent entre :

- ◆ **706 cartes pour le régime des mines.** Toutefois, s'agissant d'un régime fermé (pas de nouveaux entrants) avec une moyenne d'âge très supérieure à 80 ans, les effets de régularisation des décès produisent des effets puissants⁸. Ainsi, **au 31 décembre 2022, le régime ne comptabilisait déjà plus de carte surnuméraire ;**
- ◆ **226 cartes pour le régime de l'Assemblée nationale** qui vient d'engager un travail de rapprochement de ses bases et de celles du GIE SESAM-Vitale concernant ses affiliés ;
- ◆ **17 cartes pour le régime du Sénat**, qui a engagé un travail de fiabilisation de ses cartes valides de ses bases en 2021, travail qui se poursuit actuellement⁹.

Tableau 3 : Comparaison entre le nombre de porteurs potentiels de cartes Vitale de plus de 16 ans et le nombre de carte Vitale par régime au 30 septembre 2022

Régime	Nombre de porteurs potentiels de 16 ans et + ¹⁰	Nombre de cartes Vitale valides ¹¹	Cartes surnuméraires	Cartes valides/Porteurs potentiels
01- Régime Général et absorbés	52 991 881	50 803 527	-	96%
02- Régime Agricole – MSA	2 726 269	2 723 952	-	100%
04- S.N.C.F	346 132	343 018	-	99%
05- R.A.T.P	84 861	82 728	-	97%
06- ENIM (Marine)	80 270	77 060	-	96%
07- Mines	81 241	81 947	706	101%
08- Militaires de Carrière	661 868	632 061	-	95%
10- Clercs, Employés de Notaire	108 585	106 905	-	98%
14- Assemblée Nationale	4 923	5 149	226	105%
15- Sénat	3 530	3 547	17	100%
90- C.A.V.I.M.A.C. (cultes)	41 773	36 219	-	87%
91- M.G.E.N	2 610 919	2 552 284	-	98%
93- Mutuelle Générale Police	118 448	116 714	-	99%
99- Autres mutuelles	449 366	432 584	-	96%
Tous régimes	60 310 066	57 997 695	949	-
Hors Cnam	7 318 185	7 194 168	-	-

Source : CNAM.

Afin de compléter cette analyse portant sur le solde global de cartes par régime, la mission a obtenu pour le régime général (52,3 millions d'assurés porteurs potentiels de cartes Vitale) le **détail des soldes par tranches d'âge entre 0 et 100 ans.**

⁸ Le régime comprenait 86 014 assurés fin décembre 2021 contre 79 540 fin décembre 2022.

⁹ Le régime du Sénat fait état de trois situations principales pouvant conduire à l'existence de cartes surnuméraires : les étudiants (ayant-droit du régime du Sénat devant s'affilier au régime général), cette situation étant en théorie réglée dorénavant dans le cadre des mutations de régime ; les personnes décédées sans que le régime ait connaissance de ce décès ; les départs à l'étranger sans que le régime ait connaissance de ce départ.

¹⁰ Source : RNIAM.

¹¹ Source : GIE SESAM-Vitale.

Annexe II

Les données établies par la CNAM en date du 24 mars 2023 font apparaître un **solde négatif de cartes Vitale valides par rapport au nombre de porteurs potentiels pour chacune des tranches d'âges considérées séparément**. Cela conduit à écarter l'hypothèse d'un solde positif pour certaines classes d'âge qui aurait été compensé par le solde négatif d'autres classes d'âge, notamment chez les personnes ayant entre 16 et 20 ans (une part des jeunes entre 16 et 18 ans étant toujours inscrits sur la carte de leurs parents en qualité d'ayants-droit).

Pour les autres régimes d'assurance maladie, faute de données disponibles par tranche d'âge équivalentes à celles du régime général, il ne peut être complètement exclu que des assurés puissent théoriquement ne pas être équipés de carte Vitale et compenser des cartes Vitale en surnombre attribuées à d'autres assurés.

1.3. Le risque de facturation sans droits au moyen de cartes Vitale invalides est limité protégeant ainsi les régimes d'assurance maladie d'éventuels préjudices financiers en cas d'utilisation de cartes surnuméraires

En termes d'enjeux financiers, l'usage d'une carte Vitale surnuméraire est non seulement très rare, mais en plus il n'engendre en pratique pas de remboursements injustifiés de l'assurance maladie.

Les cartes Vitale comportent une date de fin de droits. Celle-ci correspond à la date de mise à jour¹² à laquelle est ajoutée un an. Un professionnel de santé recevant un assuré avec une carte avec des droits échus en a alors connaissance et devrait logiquement refuser de se baser sur les droits en carte, et donc demander un paiement direct.

S'agissant des facturations :

- ◆ **depuis 2004** : la mise en place de **listes d'opposition** (cf. annexe I) empêche toute facturation à l'assurance maladie à partir des cartes Vitale qui y sont inscrites.
- ◆ en complément, pour l'ensemble des professionnels de santé, le **téléservice de consultation des droits en ligne ADRI utilisé avec une carte Vitale dans le lecteur fait un contrôle d'opposition de la carte** (cf. annexe I) ce qui permet à chaque profession d'avoir accès à la liste d'opposition ;
- ◆ enfin, les contrôles de liste d'opposition sont également faits dans les **centraux des assurances maladie lors du traitement des FSE avec** :
 - en cas de paiement vers l'assuré pour un flux hors tiers payant, un signalement déclenchant contrôle systématique et processus de récupération de la carte
 - pour un flux en tiers payant avec garantie de paiement, un signalement au professionnel de santé.

Les cartes invalidées permettent au professionnel de santé de **télétransmettre les FSE**. Le cas échéant, les règlements dus aux professionnels de santé sont honorés (**garantie de paiement associé à l'usage de la carte Vitale**). Cela explique qu'une partie des flux engendrés par ces cartes ont suscité des paiements.

Inversement, les **règlements à l'assuré sont rejetés** avec un code rejet spécifique. L'organisme de sécurité sociale :

- informe l'assuré social du non-paiement de la facture ;
- lui demande la restitution de la carte Vitale à des fins de destruction.

¹² La date de personnalisation, c'est-à-dire le jour où les données de l'assuré sont entrées dans la carte pour la première fois lors de son émission.

Annexe II

En 2020, le directeur général de la CNAM a indiqué¹³ à la commission d'enquête de l'Assemblée nationale relative à la lutte contre les fraudes aux prestations sociales que la caisse avait « étudié, sur les dernières années, les tentatives de facturation de soins utilisant des cartes Vitale qui ont ensuite été mises en opposition, parce que considérées en fin de vie ou présumées abusives, frauduleuses, inutilisables ou inexistantes.

En 2019, **330 000 feuilles de soins ont été concernées, soit 0,023 % des feuilles de soins électroniques (FSE)**. Pour plus des deux tiers, le règlement a été stoppé. Pour le tiers restant, soit environ 100 000 feuilles de soins adressées dans le cadre d'un tiers payant réalisé par un professionnel de santé, l'assurance maladie a réglé à hauteur de 4 millions d'euros au titre de la garantie de paiement (applicable dès lors qu'une carte Vitale est utilisée).

Pour autant, ces rejets signifient seulement que la carte Vitale utilisée n'était pas celle connue des services de l'assurance maladie. La question de l'existence de droits à l'assurance maladie se pose, seule leur absence permettant de conclure à une fraude. Or, le directeur général de la CNAM a indiqué¹⁴ que « sur un échantillon de 11 000 rejets liés à une carte non valide, [la CNAM a étudié] si l'assuré avait encore des droits ouverts légitimement auprès de notre organisme. C'était le cas de tous ».

Par conséquent :

- ◆ l'usage d'une carte Vitale surnuméraire est rapidement détecté par les organismes de sécurité sociale et des mesures correctives sont mises en place afin qu'elles soient détruites ;
- ◆ d'après la CNAM, en 2019, les montants déboursés par le régime général au titre d'un flux généré par une carte Vitale surnuméraire n'ont pas bénéficié à des personnes dépourvues de droits. Par conséquent, cette étude conclut à un préjudice sinon nul, du moins totalement négligeable, lié à l'utilisation de cartes Vitales surnuméraires.

¹³ Séance du 16 juin 2020, compte-rendu n°14.

¹⁴ Idem.

2. Des limites méthodologiques structurelles conduisent à un écart peu intelligible entre le nombre de ressortissants des régimes d'assurance maladie et la population légale, qui ne se correspondent pas

La population française est connue par deux outils (2.1) :

- ◆ à titre principal, le recensement, qui est issu d'une enquête statistique, permet d'établir la population légale ;
- ◆ à titre accessoire, le répertoire national d'identification des personnes physiques (RNIPP), répertoire issu de données administratives, rassemble les identités de toutes les personnes nées en France ou y ayant séjourné, pourvu qu'elles soient connues des régimes de sécurité sociale.

La population légale et la population assurée (2.2) ne correspondent pas :

- ◆ car certaines personnes résidant en France n'y sont pas assurées sociales (2.3) ;
- ◆ car, inversement, certaines personnes ne résidant pas en France y sont assurées sociales (2.4).

Ces populations sont très mal connues. En ordre de grandeur, les écarts demeurent que la qualité des données ne permet pas d'expliquer à ce stade (2.5).

2.1. La population française est connue par le recensement, mais l'INSEE gère aussi le RNIPP, qui rassemble les identités des personnes nées en France ou y ayant résidé

La population française est connue de l'INSEE au moyen du **recensement de la population**, qui établit la population légale¹⁵ française, et est obtenu après mobilisation d'une enquête statistique.

Parallèlement, l'INSEE gère le **répertoire national d'identification des personnes physiques (RNIPP)** qui rassemble les identités de toutes les personnes nées en France ou venues en France (même pour peu de temps) et connues du système de protection sociale. Le RNIPP est un répertoire obtenu sur la base des données administratives (actes d'état civil français ou étrangers). Ce répertoire irrigue les systèmes d'information des organismes de sécurité sociale français, toutes branches comprises.

Ces deux outils ne sont pas articulés : le recensement constitue une photo de la population résidant en France à un instant donné (logique de bilan ou de stock) alors que le RNIPP est issu de l'accumulation de flux entrants (logique de compte de résultat) et du flux sortant des décès (mais pas des sorties du territoire). **Ces deux bases ne sont pas réconciliées.**

¹⁵ L'existence de cette enquête est prévue par la loi : articles 156 à 158 de la loi n° 2002-276 du 27 février 2002.

2.1.1. La population légale est établie sur la base d'une enquête statistique, le recensement

Un résident en France est défini comme une personne physique, indépendamment de sa nationalité, ayant son domicile principal en France, à l'exception des militaires et fonctionnaires étrangers en poste en France¹⁶, sans considération pour la durée de leur mission. Une durée de 12 mois consécutifs de résidence est requise afin d'être comptabilisé comme résident (durée déjà effectuée ou à venir).

La population légale est estimée chaque année pour chaque commune sur la base d'une enquête statistique *ad hoc*, le recensement « permanent ». Elle est estimée car :

- ◆ les communes de moins de 10 000 habitants réalisent une enquête exhaustive (toute la population communale est recensée) une fois tous les 5 ans (les 4 autres années, la population est estimée avec des méthodes statistiques et le recours à des sources fiscales) ;
- ◆ les communes de plus de 10 000 habitants réalisent chaque année une enquête sur un échantillon représentant 8 % de la population communale, leur population est estimée avec le cumul de 5 années d'enquêtes (soit un échantillon de 40 %)

L'enquête de recensement est effectuée par les communes sous l'autorité de l'INSEE. Elle est distincte du recensement militaire prévu aux articles L. 113-1 et suivants du code du service national. Un dispositif particulier est déployé afin de recenser les gens du voyage et les personnes sans abri.

En raison de la rotation des communes concernées, l'INSEE ne publie de chiffres définitifs de population communale qu'avec un décalage de trois ans pour des raisons de qualité et d'équité entre les communes. Toutefois, des estimations de population sur des niveaux géographiques de plus grande taille (France, régions, départements), susceptibles de modifications ultérieures, sont publiées de manière plus rapide.

Encadré 1 : Les données recueillies à l'occasion du recensement

S'agissant d'une enquête statistique, des données de plusieurs types sont recueillies à l'occasion du recensement :

- évolution et structure de la population (âge, sexe...) ;
- couples-familles-ménages (état matrimonial, vie en couple, taille du ménage...) ;
- logements-migrations résidentielles (catégorie et type de logement, période d'achèvement, statut d'occupation, nombre de pièces, ancienneté d'emménagement, lieu de résidence cinq ans ou un an plus tôt...) ;
- diplômes-formation-mobilités scolaires (scolarisation et lieu d'études, diplôme le plus élevé...) ;
- population active-emploi-chômage (taux d'activité par sexe et âge, actifs en emploi, chômage au sens du recensement...) ;
- caractéristiques de l'emploi-mobilités professionnelles (statut professionnel, condition d'emploi, temps partiel, lieu de travail, mode de transport pour aller travailler...) ;
- étrangers-immigrés (distinction Français / étranger et immigré / non immigré par sexe et âge...).

¹⁶ En fait, seuls les personnels résidant dans des locaux diplomatiques sont considérés comme appartenant à la population du pays que l'ambassade représente.

Annexe II

Par échantillonnage, certaines réponses sont complétées, au besoin avec une intervention humaine, afin de produire des données plus complexes décrivant précisément :

- la structure familiale des ménages : détermination précise de la personne de référence du ménage, identification, le cas échéant, de familles au sein du ménage et composition de ces familles ;
- les secteurs d'activité dans lesquels les emplois sont exercés ;
- la profession et la catégorie socioprofessionnelle des personnes, qu'elles occupent un emploi ou en recherchent un.

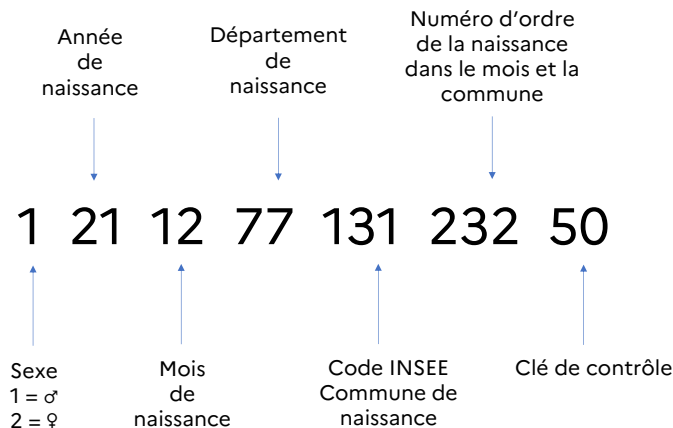
Source : mission sur la base du document « Recensement de la population – les exploitations principale et complémentaire », INSEE, juin 2022.

La population légale est authentifiée chaque année par décret. Au 1er janvier 2023, l'INSEE indiquait une population résidente estimée à 68 043 000 habitants, contre 67 843 000 au 1er janvier 2022 et 67 635 000 au 1er janvier 2021.

2.1.2. Le répertoire national d'identification des personnes physiques (RNIPP) contient aussi des informations sur la population

Tenu par l'INSEE depuis sa fondation¹⁷ en 1946, le répertoire national d'identification des personnes physiques (RNIPP), régi par les dispositions du décret n° 82-103 du 22 janvier 1982, comprend l'état-civil des personnes nées en France et des personnes nées à l'étranger et venues vivre en France dès lors qu'elles sont connues du système de protection sociale.

Dans ce répertoire, les personnes physiques sont identifiées par un numéro unique, le numéro d'inscription au répertoire (NIR), comprend 13 chiffres plus une clé de contrôle, comme indiqué dans le schéma ci-dessous :



Source : Mission.

Le NIR est attribué dès la naissance pour les personnes nées en France (en pratique, quelques jours après la naissance) et dès validation des documents d'état civil fournis à l'arrivée en France pour les personnes nées à l'étranger. Il sert d'identifiant unique aux organismes de sécurité sociale (d'où son appellation « numéro de sécurité sociale »).

Le RNIPP étant alimenté par les éléments d'état-civil, il rend compte des principaux éléments retraçant celui-ci :

- ◆ à la naissance : nom, prénoms, date et lieu (avec l'inscription au RNIPP) ;
- ◆ changement de nom ou de prénoms ;

¹⁷ Décret 46-1432 du 14 juin 1946.

Annexe II

- ◆ changement de sexe (en ce cas, le premier chiffre du NIR est modifié) ;
- ◆ décès, date et lieu.

Il comprend à titre principal les cinq traits d'identité suivants :

- ◆ nom ;
- ◆ prénoms ;
- ◆ sexe ;
- ◆ date de naissance ;
- ◆ lieu de naissance (code INSEE de la commune de naissance pour les personnes nées en France, avec toutes les difficultés liées aux fusions de commune par exemple ; code INSEE du pays de naissance pour les personnes nées à l'étranger).

Des traits d'identité secondaire (comme la filiation maternelle et paternelle) permettent de distinguer les presque 300 homonymes parfaits (partageant exactement les cinq traits d'identité) existant au sein du RNIPP pour les personnes nées en France.

Les personnes décédées n'étant pas retirées du RNIPP, celui comprenait en 2022 les données d'état-civil de plus de 113 millions de personnes vivant ou ayant vécu en France depuis sa création¹⁸. En effet, il est nécessaire de conserver l'identité des personnes décédées pour certains besoins administratifs.

S'agissant des personnes nées à l'étranger, elles suivent un processus différent : elles doivent demander à un organisme de sécurité sociale leur affiliation. Tant que leur identité n'est pas certifiée, elles se voient attribuer un numéro d'identification d'attente (NIA), construit sur le modèle du NIR (avec la différence notable que le code INSEE de la commune est remplacé par le code du pays de naissance, ce qui induit une granularité significativement plus faible et peut induire un nombre d'homonymes – partageant les cinq traits d'identité – beaucoup plus élevé que pour les personnes nées en France).

La certification de l'identité est effectuée par un service de la CNAV, le SANDIA (service administratif national d'identification des assurés). Une fois cette certification acquise, le NIA alimente le système national de gestion des identités (SNGI), géré par la CNAV, qui alimente ensuite le RNIPP. En effet, SNGI et RNIPP se synchronisent chaque nuit : le SNGI reçoit du RNIPP les informations concernant les naissances et décès de personnes nées en France ; le RNIPP reçoit du SNGI les informations concernant les assurés sociaux nés à l'étranger.

2.1.3. Les deux outils ne sont pas rapprochés ce qui peut occasionner des difficultés

Le RNIPP ne cesse de voir sa taille croître, aucune sortie du répertoire n'étant prévue. Surtout, il s'agit d'un fichier issu de données administratives recensant les personnes nées en France ou ayant été immatriculées dans le système de sécurité sociale français¹⁹ à un moment de leur vie. Il ne donne pas d'information sur la résidence de la personne considérée (notamment si des personnes sont parties à l'étranger).

Inversement, le recensement permet de connaître précisément la population résidant en France ainsi que ses principales caractéristiques socio-économiques. Toutefois, les personnes recensées ne sont pas identifiées dans ce cadre par leur NIR, dont elles peuvent d'ailleurs théoriquement être dépourvues (cf. *infra*).

¹⁸ Source : le RNIPP au cœur de la vie administrative française, Lionel ESPINASSE, Valérie ROUX, Courrier des statistiques n°8, novembre 2022.

¹⁹ Avec l'instauration du répertoire électoral unique et afin de faciliter leurs droits électoraux, les Français nés à l'étranger figurent systématiquement depuis 2022 au RNIPP même s'ils n'ont pas été affiliés à un régime de sécurité sociale français.

Annexe II

Les deux exercices ne sont donc pas articulés. Seul l'échantillon démographique permanent permet d'effectuer un lien entre les deux types de données.

Encadré 2 : L'échantillon démographique permanent

L'échantillon démographique permanent (EDP) est un échantillon de la population française, suivi aussi bien dans le cadre du recensement qu'à travers les données administratives du RNIPP.

Sont incluses dans l'EDP les personnes nées en France « du 2 au 5 janvier, du 1er au 4 avril, du 1er au 4 juillet et du 1er au 4 octobre de chaque année » (arrêté du 6 août 2014, JORF du 9 octobre 2014), soit un peu plus de 4 % de la population française.

En 2021, plus de 3,7 millions de personnes figuraient dans l'EDP, base permettant un recul de plus 50 ans (les premières inclusions datent de 1968) et comportant des informations relatives à l'état-civil (principalement issues du RNIPP), des données relatives à la vie personnelle et professionnelle ou d'ordre économique et financier (principalement issues du recensement, du fichier électoral, de données fiscales et des déclarations sociales).

L'intérêt de l'EDP est qu'il suit une tranche de la population tout au long de sa vie. Les descriptions « en coupe » peuvent ainsi prendre une dimension dynamique en permettant une description des trajectoires tout au long de la vie en termes professionnels, familiaux, de logement etc...

Source : Mission, sur la base de l'échantillon démographique permanent, en 50 ans, l'EDP a bien grandi !, Isabelle ROBERT-BOBÉE, Natacha GUALBERT, Courrier des statistiques n°6, juin 2021.

2.2. La population assurée française est connue de manière incrémentale sur la base de données administrative

Le **répertoire national inter-régimes des bénéficiaires de l'assurance maladie (RNIAM)** comportait 72 458 072 assurés au 2 janvier 2020, 72 873 222 assurés au 1^{er} janvier 2021 et 73 109 186 assurés au 1^{er} janvier 2022 disposant de droits ouverts et dont les régimes d'assurance maladie n'ont pas connaissance du décès²⁰.

Ces assurés sociaux étaient répartis en fonction de leur âge de la manière suivante :

Tableau 4 : Nombre d'assurés sociaux inscrits au RNIAM

-	Assurés de 15 ans ou moins	Assurés ayant entre 16 et 64 ans inclus	Assurés de 65 ans et plus	Total
Au 2 janvier 2020	13 081 542	36 336 508	23 040 022	72 458 072
Au 1er janvier 2021	13 020 681	36 455 836	23 396 705	72 873 222
Au 1er janvier 2022	12 940 273	36 448 209	23 720 704	73 109 186

Source : CNAM.

Or, les populations résidentes au sens de l'INSEE et les populations assurées ne se recoupent pas :

- ◆ certains résidents au sens de l'INSEE peuvent ne pas être assurés sociaux français ;
- ◆ certains assurés sociaux français peuvent ne pas être résidents au sens de l'INSEE.

²⁰ Source : CNAM.

2.3. Certaines personnes résidant en France ne sont pas assurées sociales

Des personnes résidant sur le territoire français sont susceptibles de ne pas être assurées sociales françaises :

- ◆ lorsqu'elles disposent d'un contrat de travail soumis au droit d'un pays membre – autre que la France - de l'Union européenne, et sont donc ressortissantes d'un système de sécurité sociale communautaire, mais exercent leur activité professionnelle en France dans le cadre du détachement de travailleurs communautaires ;
- ◆ lorsqu'un résident français dispose d'un contrat de travail soumis au droit d'un pays membre de l'Union européenne (frontalier communautaires) ;
- ◆ lorsqu'un résident français dispose d'un contrat de travail soumis au droit helvétique, en fonction de son exercice ou non du droit d'option à l'assurance maladie suisse (frontaliers suisses) ;
- ◆ les étudiants communautaires en échange ERASMUS pour une durée limitée ;
- ◆ certains résidents de communautés d'outre-mer²¹ .

2.3.1. Certains travailleurs détachés entrants peuvent relever de régimes de sécurité sociale étrangers

Les travailleurs détachés entrants sont, par définition du détachement au sens communautaire²², ressortissants du système de sécurité sociale de leur pays d'origine, mais exercent leur activité professionnelle en France.

Cette activité est nécessairement limitée dans le temps, mais elle peut s'étendre, en fonction des accords bilatéraux, jusqu'à six ans. Ainsi, en fonction de la durée de détachement, le travailleur peut ou non être comptabilisé dans la population française. Par ailleurs, si le travailleur détaché est muni d'un formulaire S1 (fourni par le régime de sécurité sociale du pays d'origine, et donc après accord de celui-ci), le travailleur détaché est immatriculé à la sécurité sociale française en tant que travailleur salarié de droit commun et peut bénéficier à ce titre d'une carte Vitale.

De manière générale, le travail détaché est régi par les dispositions du règlement n° 88 /2004. Ce texte prévoit :

- ◆ de principe, une durée de détachement inférieure à 24 mois (article 12.1 d règlement n° 883/2004) ;
- ◆ par dérogation, une durée supérieure de détachement peut être accordée dans le cadre de conventions bilatérales entre États membres (article 16 du règlement n° 883/2004). Ces dérogations demeurent marginales. Ainsi, en 2021, 587 accords ont été formulés dans ce cadre²³.

Leur nombre prête à discussion²⁴, d'autant que les éléments de durée (12 mois de présence sur le territoire sont nécessaires pour être recensé comme résident en France). Toutefois, s'agissant de la réglementation de la sécurité sociale, la mission retiendra le chiffre fourni par le CLEISS²⁵, soit 257 338 détachements entrants en 2021.

²¹ La protection sociale ne faisant pas partie des compétences intransférables aux communautés d'outre-mer en application des dispositions combinées des articles 74 et 73 de la Constitution.

²² Le Liechtenstein, la Norvège et l'Islande sont considérés comme des pays communautaires dans ce cadre.

²³ Source : CLEISS, rapport statistique 2021, page 66.

²⁴ Voir notamment le rapport IGAS n°2020-086 de mars 2021.

²⁵ Source : CLEISS, rapport statistique 2021, page 70.

2.3.2. Les travailleurs frontaliers communautaires sortants ne relèvent généralement pas de la sécurité sociale française

Il s'agit des personnes résidant en France et, ayant leur activité professionnelle dans un pays communautaire frontalier (Belgique, Luxembourg, Allemagne, Italie ou Espagne²⁶), qui sont affiliées au système de sécurité sociale de ces pays.

Encadré 3 : La nuance entre travailleur frontalier et travailleur transfrontalier

En application du f) de l'article 1^{er} du règlement n° 883/2004 l du 29 avril 2004 sur la coordination des systèmes de sécurité sociale, un travailleur frontalier est une « *personne qui exerce une activité salariée ou non salariée dans un État membre et qui réside dans un autre État membre où elle retourne en principe chaque jour ou au moins une fois par semaine* ».

Un travailleur transfrontalier est titulaire d'un emploi dans un pays distinct du pays dans lequel il réside, sans nécessairement traverser quotidiennement la frontière : le critère de fréquence du passage de la frontière (idéalement quotidien et au moins hebdomadaire pour les travailleurs frontaliers) est relâché dans ce cas.

Source : Mission.

Dans ce cas, ce sont les dispositions communautaires qui s'appliquent :

- ◆ le règlement n°883/2004 du Parlement Européen et du Conseil du 29 avril 2004 portant sur la coordination des systèmes de sécurité sociale, ainsi que son règlement d'application n°987/2009 ;
- ◆ le règlement n°1408/71 du Conseil, du 14 juin 1971, relatif à l'application des régimes de sécurité sociale aux travailleurs salariés, aux travailleurs non-salariés et aux membres de leur famille qui se déplacent à l'intérieur de la Communauté ainsi que son règlement d'application n°574/72.

Dans ce cas, ces résidents français au sens de l'INSEE ne sont pas assurés sociaux français, la sécurité sociale étant ici prise de manière indivisible à l'exception de la dépendance (c'est-à-dire pour l'ensemble des risques – famille, vieillesse, maladie, accidents du travail et maladie professionnelle).

2.3.3. Certains travailleurs frontaliers avec la Suisse y sont affiliés pour le risque maladie

Le cas des travailleurs frontaliers suisses est proche du cas des travailleurs frontaliers communautaires, avec une différence significative : les travailleurs résidant en France et travaillant en Suisse disposent d'une option leur permettant de choisir entre :

- ◆ le système d'assurance maladie suisse, leur cas s'apparentant alors à celui des frontaliers communautaires ;
- ◆ le système d'assurance maladie français, leur cas s'apparentant alors à celui des résidents français travaillant en France.

Cette option ne couvre que les prestations en nature du risque maladie²⁷. Pour les autres risques, ces personnes demeurent affiliées dans leur État d'emploi (la Suisse).

²⁶ Il conviendrait d'ajouter les Pays-Bas. Toutefois des dispositions particulières sont applicables à l'île de Saint-Martin. En toute hypothèse, les effectifs concernés ne sont pas suffisants pour expliquer, en tout ou partie, les écarts constatés de manière significative.

²⁷ CSS, art. L. 380-3-1.

Annexe II

Le même droit d'option est en outre offert aux retraités percevant une pension suisse et venant résider en France.

2.3.4. Les étudiants étrangers du programme ERASMUS demeurent en principe affiliés à leur régime d'origine

Les étudiants étrangers étudiant en France dans le cadre du programme ERASMUS demeurent en principe assurés sociaux de leur pays d'origine. Toutefois, lorsque leurs études dépassent une certaine durée (12 mois), ils sont considérés par l'INSEE comme des résidents français.

Sans considération pour la durée de séjour²⁸, en 2021, la France a accueilli 25 653 étudiants et enseignants dans le champ « *higher education* » et 2 469 dans le champ « *vocational education and training* ».

2.3.5. Certains territoires français non couverts par l'assurance maladie permettent la couverture de leurs ressortissants par cette dernière

Les résidents de certains territoires français ne sont pas assujettis à la sécurité sociale française mais sont ressortissants d'un système local d'assurance maladie. Dans certains cas, un accord a été passé entre la communauté d'outre-mer (COM) et la République française visant à la prise en charge par la sécurité sociale française des ressortissants des systèmes locaux d'assurance maladie :

- ◆ Nouvelle Calédonie : accord du 9 novembre 2002. En 2019, la population de la Nouvelle-Calédonie était de 271 400 habitants selon l'INSEE²⁹ ;
- ◆ Polynésie française : accord du 26 décembre 1999. En 2017, la population de la Polynésie française était de 275 900 habitants selon l'INSEE³⁰ ;
- ◆ Saint-Pierre et Miquelon : accord du 10 mai 2011.

Par ailleurs, les habitants de Wallis et Futuna sont affiliés à la CPAM de Paris³¹ et se voient remettre une attestation de droits. Ils bénéficient de l'émission d'une carte Vitale en cas d'évacuation sanitaire vers la métropole (article 5-1 de la convention). La population de Wallis et Futuna était de 11 600 habitants en 2018 selon l'INSEE³².

Ainsi, par défaut, la population des COM n'est en théorie pas couverte par l'assurance maladie française, nonobstant certains accords permettant leur affiliation, au cas par cas, à celle-ci.

Ce sont donc au plus 500 000 personnes qui sont résidentes en France mais non affiliées à la sécurité sociale française.

2.4. Inversement, certains assurés sociaux peuvent ne pas résider en France

De nombreux cas de figure d'assurés sociaux non-résidents existent :

²⁸ Source : Commission européenne, Direction générale de l'éducation, de la jeunesse, du sport et de la culture, Erasmus+ annual report 2021 : statistical annex, Office des publications de l'Union européenne, 2022 (document indisponible en français).

²⁹ Source : INSEE Première n°1823, 29 octobre 2020.

³⁰ Source : INSEE Première n°1721, 30 novembre 2018.

³¹ Convention du 23 février 2017 liant l'assurance maladie d'une part et l'Agence territoriale de santé de Wallis et Futuna d'autre part.

³² Source : INSEE Première n°1775, 26 septembre 2019.

Annexe II

- ◆ certains travailleurs français détachés dans un État membre de l'Union européenne, sous certaines conditions de durée ;
- ◆ certains titulaires d'une pension vieillesse, invalidité ou inaptitude résidant à l'étranger ;
- ◆ certains étudiants français du programme ERASMUS ;
- ◆ certains étudiants étrangers hors programme ERASMUS ;
- ◆ les travailleurs saisonniers ;
- ◆ certains résidents dans un pays étranger, en vertu d'accords bilatéraux.

2.4.1. Les travailleurs détachés sortants demeurent en principe affiliés en France

De manière symétrique au cas des travailleurs détachés entrants vus *supra*, les travailleurs détachés sortants sont ressortissants du système de sécurité sociale français, mais peuvent être, lorsque le détachement est d'une durée significative, des résidents étrangers et donc ne pas apparaître dans la population française.

D'après le CLEISS³³, « en 2021, la France a délivré 120 462 formulaires, attestant d'un maintien d'affiliation à la législation française de sécurité sociale, à ses travailleurs en situation de détachement à l'étranger ». Parmi ceux-ci, 99 089 détachements concernaient des pays de l'Union européenne³⁴. Sans précision de la durée, ce chiffre est un majorant.

2.4.2. Les titulaires d'une pension de vieillesse, d'invalidité ou d'inaptitude française et résidant à l'étranger bénéficient de la prise en charge de leurs frais de santé

L'article L. 160-3 du code de la sécurité sociale prévoit que des personnes résidant à l'étranger bénéficient lors de séjours temporaires en France de la prise en charge de leurs frais de santé correspondant à des prestations en nature dans les cas suivants :

- ◆ les pensionnés, qu'ils soient titulaires d'un droit direct ou de réversion, d'un régime obligatoire d'assurance vieillesse français ;
- ◆ les titulaires d'une pension d'invalidité de la branche AT/MP (hors professions agricoles) ;
- ◆ les titulaires d'une pension de vieillesse accordée en substitution d'une pension d'invalidité (cas de la retraite pour inaptitude) ;
- ◆ aux titulaires de la prestation d'aide à la vie familiale et sociale prévue à l'article L. 117-3 du code de l'action sociale et des familles.

Pour pouvoir bénéficier de cette mesure, il faut :

- ◆ que la France soit l'État exclusivement compétent au regard de règles prévues par les conventions internationales de sécurité sociale (voir encadré) ;
- ◆ ou que « la pension rémunère une durée d'assurance supérieure ou égale à quinze années au titre d'un régime français ». Toutefois, l'article 92 de la loi n° 2021-1754 du 21 décembre 2021 (loi de financement de la sécurité sociale pour 2022) a élargi le bénéfice de l'article L. 160-3 aux personnes qui « bénéficiaient, lors de leurs séjours temporaires en France, de la prise en charge de leurs frais de santé avant le 1^{er} juillet 2019 [...] dès lors que leur pension rémunère une durée d'assurance supérieure ou égale à dix années au titre d'un régime français de sécurité sociale ».

³³ CLEISS, rapport statistique 2021, page 60.

³⁴ Plus l'EEE, la Suisse et le Royaume-Uni.

Annexe II

Au 31 décembre 2020, les régimes de retraites français versaient des pensions de droit direct ou dérivé à 17,9 millions de personnes, dont 1,6 millions résidaient à l'étranger³⁵.

Encadré 4 : La définition de l'État membre compétent en droit communautaire

En application du s) de l'article 1er du règlement n° 883/2004 l du 29 avril 2004 sur la coordination des systèmes de sécurité sociale, l'État membre compétent est « l'État membre dans lequel se trouve l'institution compétente ».

Le q) du même article définit l'institution compétente comme :

- soit « l'institution à laquelle l'intéressé est affilié au moment de la demande de prestations » ;
- soit « l'institution de la part de laquelle l'intéressé a droit ou aurait droit à des prestations s'il résidait ou si le ou les membres de sa famille résidaient dans l'État membre où se trouve cette institution » ;
- soit « l'institution désignée par l'autorité compétente de l'État membre concerné »

Source : Mission.

2.4.3. Les étudiants étrangers étudiant en France relèvent de la sécurité sociale française sans nécessairement être résidents français

Les étudiants français étudiant à l'étranger dans le cadre du programme ERASMUS demeurent en principe assurés sociaux français. Lorsqu'ils sont présents à l'étranger plus d'une certaine durée (24 mois), ils cessent d'être considérés par l'INSEE comme des résidents français.

Par ailleurs, s'agissant des étudiants hors Union européenne, ils ne sont pas considérés comme résidents français lorsque leur séjour est court (moins de deux ans) ; toutefois, ils sont affiliés à la sécurité sociale à l'occasion de leur arrivée sur le territoire et y maintiennent des droits (dans le cadre de la protection universelle maladie - PUMA) jusqu'à l'expiration de leur visa.

En 2021, près de 80 000 visas pour études ont été délivrés³⁶.

2.4.4. Les étudiants français du programme ERASMUS étudiant à l'étranger relèvent de la sécurité sociale française sans nécessairement être résidents en France

Par symétrie avec la situation des étudiants étrangers venant en France dans le cadre du programme ERASMUS, les étudiants français étudiant à l'étranger demeurent ressortissants de la sécurité sociale française malgré leur séjour à l'étranger. En fonction de la durée de celui-ci, ils sont comptabilisés dans la population française (séjour court) ou non (séjour supérieur à un an).

Pour mémoire, le GIP Agence Erasmus+ France/Éducation Formation a communiqué à la mission, en ordre de grandeur, les flux sortants d'étudiants du programme ERASMUS.

Tableau 5 : Flux sortant d'étudiants du programme ERASMUS 2020-2022

Type de mobilité	Année scolaire 2020/21	Année scolaire 2021/22
Études	24 000	28 500
Stages	11 500	14 500
Total	35 500	43 000

Source : Agence Erasmus+ France/Education Formation (chiffres non consolidés – ordres de grandeur).

³⁵ Source : DREES, Les retraités et les retraites, édition 2022.

³⁶ Sur la période allant du 1^{er} janvier au 31 octobre (en lien avec l'année scolaire). Source : Campus France, Chiffres clés, La mobilité étudiante dans le monde, juin 2022.

2.4.5. Les travailleurs saisonniers ne sont pas résidents français mais ont des droits à l'assurance maladie française

Les travailleurs saisonniers titulaires d'une carte de séjour pluriannuelle³⁷ portant la mention « saisonnier » exercent leur activité en France pour une durée ne dépassant pas 6 mois par an. Les titulaires de cette carte de séjour doivent en outre s'engager à maintenir leur domicile habituel à l'étranger. Cette carte de séjour, d'une durée maximale de trois ans, est renouvelable.

Les porteurs de ce titre de séjour sont titulaires de droits à l'assurance maladie, en application de l'article L. 111-2-2 du code de la sécurité sociale qui prévoit l'affiliation, sans condition de résidence³⁸, des personnes exerçant en France une activité salariée ou non salariée.

En 2021, 6 740 premiers titres de séjour ont été accordés sur cette base³⁹. En supposant que tous les titres aient une durée de trois ans (hypothèse maximaliste) mais qu'ils ne soient jamais renouvelés (hypothèse minimaliste), ce seraient environ 20 000 personnes qui seraient ainsi affiliées à la sécurité sociale française sans être résidents.

2.4.6. En fonction des conventions bilatérales, les résidents de certains pays peuvent voir pris en charge leurs frais de santé par la sécurité sociale française

En sus du cadre communautaire, il existe des conventions avec plusieurs pays, prévoyant la prise en charge, sous des conditions stipulées dans chaque accord, de tout ou partie des prestations d'assurance maladie⁴⁰. Il existe des conventions avec les pays et collectivités étrangères suivants :

- ◆ Algérie : convention générale du 1^{er} octobre 1980, pour le travailleur et sa famille lorsqu'elle accompagne le travailleur ;
- ◆ Andorre : convention du 12 décembre 2000 ;
- ◆ Bénin : convention et protocole n°1 du 6 novembre 1979, pour le seul risque maternité ;
- ◆ Bosnie-Herzégovine : accord de 2003, pour le travailleur et sa famille lorsqu'elle accompagne le travailleur ;
- ◆ Cap-Vert : convention générale du 15 janvier 1980, pour le travailleur et sa famille lorsqu'elle accompagne le travailleur ;
- ◆ Gabon : accord du 2 octobre 1983, pour le travailleur et sa famille lorsqu'elle accompagne le travailleur ;
- ◆ Guernesey et Jersey : convention franco-britannique du 10 juillet 1999 et accord du 29 mai 1979, pour l'hospitalisation d'urgence du travailleur et de sa famille ;
- ◆ Kosovo : accord de 2013 pour le travailleur et sa famille lorsqu'elle accompagne le travailleur ;
- ◆ Macédoine du nord : accord de 1995, pour le travailleur et sa famille lorsqu'elle accompagne le travailleur ;
- ◆ Mali : convention générale du 12 mai 1979, pour le seul risque maladie du travailleur et de sa famille lorsqu'elle accompagne le travailleur ;

³⁷ Article L. 421-34 du code de l'entrée et du séjour des étrangers et du droit d'asile.

³⁸ Mais avec une condition de régularité du séjour (CSS, art. L. 115-6), remplie par hypothèse dans ce cas).

³⁹ Source : Ministère de l'intérieur, Direction générale des étrangers en France, Département des statistiques, des études et de la documentation, *L'essentiel de l'immigration* n° 2022-75, janvier 2022.

⁴⁰ Des conventions bilatérales existent également, pour d'autres risques que la maladie, avec les États suivants : Argentine, Brésil, Cameroun, Canada (hors Québec), Chili, Congo Brazzaville, Corée du sud, Côte d'Ivoire, États-Unis d'Amérique, Inde, Israël, Japon, Madagascar, Mauritanie, Philippines, Saint-Marin, Sénégal et Uruguay.

Annexe II

- ◆ Maroc : convention générale du 22 octobre 2007, pour le travailleur et sa famille lorsqu'elle accompagne le travailleur ;
- ◆ Monaco : convention générale du 28 février 1954, pour le travailleur et sa famille ;
- ◆ Monténégro : accord du 26 mars 2003, pour le travailleur et sa famille lorsqu'elle accompagne le travailleur ;
- ◆ Niger : convention générale et protocole du 28 mars 1973, pour le seul risque maternité du travailleur ;
- ◆ Québec : entente du 17 décembre 2003 ;
- ◆ Serbie : accord du 26 mars 2003 pour le travailleur et sa famille lorsqu'elle accompagne le travailleur ;
- ◆ Togo : convention générale et protocole n°1 du 1^{er} juillet 1973, pour le seul risque maternité du travailleur ;
- ◆ Tunisie : convention générale du 26 juin 2003, pour le travailleur et sa famille lorsqu'elle accompagne le travailleur ;
- ◆ Turquie : convention générale du 20 janvier 1972, pour le travailleur.

2.5. Un écart entre la population assurée et la population résidente demeure

L'écart entre la population affiliée à l'assurance maladie et la population résidente sur le territoire apparaît difficile à expliquer. Au 1^{er} janvier 2020, la CNAM indiquait un « **écart brut** » sur l'ensemble de la population de **5,4 millions de personnes** en rattachement dans les organismes d'assurance maladie constaté entre les données de l'INSEE et celles du RNIAM.

En effet, en théorie, la population affiliée est égale à la population résidente :

- ◆ à laquelle on retranche la population résidente non assurée sociale, soit :
 - certains travailleurs détachés entrants soit au plus 250 000 personnes ;
 - les travailleurs transfrontaliers avec la Suisse n'ayant pas opté pour l'assurance maladie française (compris dans le compte des travailleurs détachés sortants) ;
 - les travailleurs frontaliers résidant en France et travaillant à l'étranger : ce nombre est impossible à estimer, mais on peut faire l'hypothèse simplificatrice⁴¹ qu'ils sont en nombre égal aux travailleurs frontaliers résidant à l'étranger et travaillant en France ;
 - certains étudiants du programme ERASMUS, soit tout au plus 30 000 personnes.
 - certains citoyens français résidant Outre-mer (Nouvelle-Calédonie, Saint-Pierre et Miquelon, Polynésie française, Wallis et Futuna, Saint Barthélémy et Saint Martin), soit environ 500 000 personnes ;
- ◆ et à laquelle on ajoute :
 - certains travailleurs détachés sortant soit au plus 50 000 personnes ;
 - les travailleurs frontaliers résidant à l'étranger et exerçant en France ;
 - certains étudiants français du programme ERASMUS soit au plus 40 000 personnes ;
 - certains étudiants étrangers hors programme ERASMUS, soit au plus 80 000 personnes ;
 - les travailleurs saisonniers, soit de l'ordre de 20 000 personnes ;

⁴¹ Cette hypothèse est très discutable, les bassins d'emploi et niveaux de salaire n'étant pas symétriquement situés en France et à l'étranger.

Annexe II

- certains résidents dans un pays étranger, qui bénéficient d'une prise en charge par l'assurance maladie, soit environ 1,6 million de personnes.

En conclusion, même en tenant compte de la fragilité du chiffrage obtenu, **il demeurerait un « stock » d'assurés sociaux non-résidents de plus de 4 millions de personnes avec des incertitudes très fortes sur les chiffres.**

La CNAM, dans des travaux conduits en 2020, a recherché les éléments explicatifs de cet écart :

- ◆ certaines personnes s'assurent à la Caisse des Français de l'étranger, et ne sont donc pas résidentes, tout en étant affiliées de manière volontaire à la sécurité sociale française (environ 200 000 personnes) ;
- ◆ la CNAM estime à 600 000 personnes les saisonniers issus de l'Union européenne. On retrouve ici le débat sur l'écart entre le nombre de personnes résidant en France mais travaillant à l'étranger et les personnes résidant à l'étranger mais travaillant en France (dont, d'après la CNAM, 600 000 saisonniers) ;
- ◆ inversement, en diminution du nombre d'assuré, la CNAM estime que le RNIAM comprend :
 - 1,1 million de personnes dont les droits ont pris fin, situation non retranscrite dans le RNIAM ;
 - 270 000 personnes avec un rattachement « obsolète » (résultant du rattachement des assurés issus de divers régimes – étudiants, indépendants, fonctionnaires, chambre de commerce et d'industrie de Paris... - au régime général) ;
 - 390 000 personnes décédées, avec décès non encore certifié ;
 - Entre 250 000 et 500 000 personnes dont le titre de séjour a expiré et qui ne peuvent en principe plus être affiliées à la sécurité sociale⁴² ;
- ◆ le nombre d'étudiants ayant quitté le territoire sans rendre leur carte Vitale s'élèverait à 270 000. Ce chiffre ne correspond pas à la situation de grande difficulté d'affiliation des étudiants étrangers décrite par CampusFrance dans son échange avec la mission.

Pour la CNAM, l'essentiel de l'écart constaté peut être donc expliqué par :

- ◆ la différence de périmètres entre le recensement INSEE et la gestion des droits maladie ;
- ◆ par des mises à jour des référentielles assurances maladie insuffisamment complètes ou réactives.

Les retraitements par la CNAM conduisent à **un écart entre les deux bases réduit à 460 000 personnes**. L'analyse de la CNAM rejoint partiellement celle de la mission : un nombre significatif de personnes (entre un et deux millions) figurerait ainsi au RNIAM sans réelle justification.

Certaines hypothèses complémentaires peuvent être avancées :

- ◆ la sécurité sociale en général et l'assurance maladie en particulier ont été conçues pour couvrir les personnes, d'où des procédures d'affiliation relativement simples (droits ouverts en raison de la résidence en France depuis la PUMa, ou en raison de l'activité professionnelle en France). Inversement, étant données les conséquences pour les personnes intéressées, la radiation est relativement compliquée à mettre en œuvre ;
- ◆ en particulier, l'affiliation au titre de la résidence pose question. Les pièces probantes permettant de justifier de celle-ci sont larges : une caisse primaire a ainsi mentionné qu'elle était tenue de prononcer l'affiliation sur de simples attestations d'hébergement.

⁴² CSS, art. L. 115-6. L'article L. 111-1 dispose que la sécurité sociale « assure, pour toute personne travaillant ou résidant en France de façon stable et régulière, la couverture des charges de maladie, de maternité et de paternité ainsi que des charges de famille et d'autonomie ».

Annexe II

En tout état de cause, avec d'importantes approximations structurelles dans les données existantes sur les populations résidentes et assurées, l'exploration de l'écart entre les deux dénombrements semble aporétique.

Dans le cadre de la lutte contre la fraude, la question de l'affiliation et de la radiation des assurés sociaux, en particulier lorsque leurs droits ne sont pas issus de cotisations plus facilement vérifiables que l'établissement durable sur le territoire, est prioritaire.

ANNEXE III

La lutte contre la fraude aux prestations d'assurance maladie et la fraude liée à l'usage des cartes Vitale

SOMMAIRE

1. SI LA FRAUDE DÉTECTÉE CHAQUE ANNÉE EST PROCHE DE 0,1% DES MONTANTS REMBOURSÉS PAR L'ASSURANCE MALADIE, DES TRAVAUX INNOVANTS CONDUITS DEPUIS 2020 DEVRAIENT PERMETTRE DE MIEUX ÉVALUER SON AMPLEUR, D'UNE ÉCHELLE BIEN SUPÉRIEURE	1
1.1. Les montants de fraude détectée et empêchée, dont la progression constante a été interrompue par la crise sanitaire, représentent environ 0,1 % des dépenses effectuées chaque année au titre de l'assurance maladie.....	1
1.2. Les premiers travaux d'estimation de la fraude lancés en 2020 sont encore incomplets mais font apparaître un niveau de fraude entre cinq et vingt fois supérieur à la fraude détectée selon les professions de santé	8
1.2.1. <i>La CNAM a fait le choix de méthodes statistiques éprouvées par d'autres organismes de sécurité sociale et par les administrations afin d'évaluer l'ampleur de la fraude</i>	<i>8</i>
1.2.2. <i>Des résultats partiels qui font apparaître un niveau de fraude élevé au sein des professions de santé examinées, entre 5% et 7% chez les infirmiers libéraux.....</i>	<i>12</i>
1.3. La fraude des assurés et des professionnels de santé peut impliquer l'utilisation de la carte Vitale sans toutefois que ne soit identifiée par l'Assurance maladie une fraude de grande ampleur spécifique à ce support.....	16
1.3.1. <i>La définition de la fraude par l'Assurance maladie inclut les détournements d'usage de la carte Vitale mais ce grief ne représente que 24 dossiers depuis 2018 pour un préjudice total cumulé inférieur à 45 000€.....</i>	<i>16</i>
1.3.2. <i>La carte Vitale peut constituer un mode opératoire dans d'autres types de fraudes, commises par des assurés et des professionnels de santé, en premier lieu les facturations d'actes fictifs.....</i>	<i>17</i>
2. LA LUTTE CONTRE LA FRAUDE PAR L'ASSURANCE MALADIE S'EST RENFORCÉE À PARTIR DE 2010, CONDUISANT À UNE HAUSSE DES MONTANTS DÉTECTÉS ET RECOUVRÉS, MAIS DES MARGES DE PROGRESSION SUBSISTENT.....	20
2.1. Approfondissant la démarche initiée en 2010, la convention d'objectifs et de gestion (COG) 2018-2022 conclue par l'État avec l'Assurance maladie a été marquée par un renforcement de la politique de lutte contre la fraude, malgré des objectifs modestes quant aux montants de fraude détectée.....	20
2.1.1. <i>Le cadre de lutte contre la fraude défini s'est renforcé au fil des COG depuis 2010, pour atteindre un objectif de 265 M€ de fraude détectés ou évités en 2022</i>	<i>20</i>
2.1.2. <i>Une prise en compte améliorée du risque de fraude, centrée sur des programmes annuels de contrôle nationaux et locaux.....</i>	<i>22</i>
2.1.3. <i>La CNAM a fait évoluer son organisation dédiée à la lutte contre la fraude et a maintenu les moyens humains dédiés autour de 2% des effectifs</i>	<i>25</i>

2.2. Le renforcement de la détection de la fraude s'est appuyé sur l'élaboration de cartographie des risques.....	27
2.3. Des mesures ont été prises depuis 2004 pour réduire les risques de délivrance frauduleuse de cartes Vitale	29
2.4. Un renforcement récent des systèmes d'information, conçus en interne à l'Assurance maladie, a été opéré afin de faciliter la détection et l'investigation des fraudes.....	29
2.4.1. <i>Le croisement des bases de données de la CNAM avec celles d'autres administrations est un outil puissant, notamment pour lutter contre la fraude à l'identité et à la résidence.....</i>	31
2.4.2. <i>La mobilisation des task force nationales en cas de fraudes à forts enjeux.....</i>	32
2.4.3. <i>L'utilisation des données par « datamining » et l'emploi récent de modélisations « machine learning » et d'algorithmes de reconnaissance vont permettre d'améliorer la détection des profils de fraudeurs.....</i>	33
3. PISTES D'AMÉLIORATION DE LA LUTTE CONTRE LA FRAUDE À L'ASSURANCE MALADIE, POUR LES TYPES DE FRAUDE IMPLIQUANT L'USAGE DE LA CARTE VITALE	34
3.1. Renforcer les initiatives déjà lancées par la CNAM dans le COG 2018-2022	35
3.1.1. <i>Mieux sécuriser l'affiliation des assurés sociaux en amont des prestations.....</i>	35
3.1.2. <i>Des contrôles automatisés a priori devraient être opérationnels à compter de 2023 dans le cadre du projet METEORE.....</i>	36
3.1.3. <i>Poursuivre l'effort de professionnalisation des équipes dédiées à la lutte contre la fraude et renforcer la diversité des profils recrutés pour s'adapter aux nouveaux enjeux de la fraude.....</i>	37
3.1.4. <i>Renforcer les échanges d'information avec les autres acteurs publics, notamment pour les processus d'immatriculation et d'identification, contrôle de l'existence et certifications des droits, contrôle de la condition de résidence et de ressources.....</i>	38
3.2. Renforcer l'usage des outils numériques de vérification des droits et poursuivre les chantiers de numérisation des prescriptions.....	41
3.2.1. <i>Afin d'éviter le versement de sommes à tort sur la base des droits ouverts en carte, la consultation des droits sur les bases ADRI et CDRI pourrait être rendue systématique par le biais du développement de l'application carte Vitale et d'une obligation conventionnelle.....</i>	41
3.2.2. <i>Tenir le calendrier de déploiement des « ordonnances numériques » prévu jusqu'à fin 2024 pour lutter contre le trafic de médicaments.....</i>	41
3.2.3. <i>Compléter la sécurisation des feuilles de soins électroniques, en imposant leur horodatage.....</i>	42

Annexe III

Afin d'appréhender les modalités et l'ampleur de la fraude sociale liée à l'usage des cartes Vitale, la mission a retenu le **périmètre du régime général de l'assurance maladie**, excluant les autres régimes d'assurance maladie obligatoire (AMO) et l'ensemble des régimes d'assurance maladie complémentaire (AMC). En l'absence de précision, les données présentées dans cette annexe se rapportent donc au régime général d'assurance maladie.

1. Si la fraude détectée chaque année est proche de 0,1% des montants remboursés par l'Assurance maladie, des travaux innovants conduits depuis 2020 devraient permettre de mieux évaluer son ampleur, d'une échelle bien supérieure

1.1. Les montants de fraude détectée et empêchée, dont la progression constante a été interrompue par la crise sanitaire, représentent environ 0,1 % des dépenses effectuées chaque année au titre de l'assurance maladie

Au cours de la période 2015-2020, **le montant des prestations servies par le régime général d'assurance maladie a progressé chaque année, passant de 159,9 milliards d'euros en 2015 à 219,9 milliards d'euros en 2020** (cf. graphique 1), soit une augmentation de 37,5%, du fait notamment d'une évolution du périmètre du régime général suite à l'intégration du régime social des indépendants au 1^{er} janvier 2018¹ et du régime étudiant au 1^{er} septembre 2019².

Les prestations servies par le régime général d'assurance maladie représentaient ainsi 9,6% du PIB de la France en 2020³, soit 74% des dépenses totales de santé (284,5 Mds€, soit 12,4 % du PIB⁴).

¹ Le régime social des indépendants (RSI) a été supprimé le 1er janvier 2018, ses missions ont été progressivement intégrées au sein du régime général de la sécurité sociale sur une période transitoire de 2 ans. En 2016, lors de l'avant dernier exercice du régime, 8,6 milliards d'euros de prestations avaient été versées par le RSI.

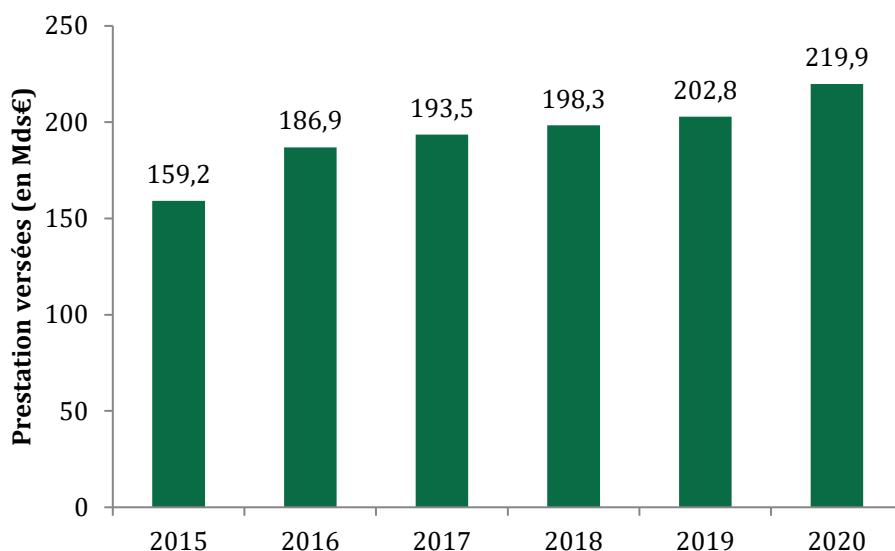
² Depuis le 1^{er} septembre 2019, les étudiants qui étaient affiliés à une mutuelle étudiante ont basculé vers le régime général et sont rattachés à la Caisse primaire d'Assurance Maladie (CPAM) de leur lieu de résidence.

³ Le PIB de la France en 2020 était de 2 300 milliards d'euros (données INSEE).

⁴ Dépense courante de santé au sens international (DCSi), établie par la DREES. La DCsi exclut les dépenses d'investissements et les revenus de remplacement (indemnités journalières).

Annexe III

Graphique 1 : Prestations nettes versées par le régime général d'assurance maladie, entre 2015 et 2020 (en milliards d'euros)

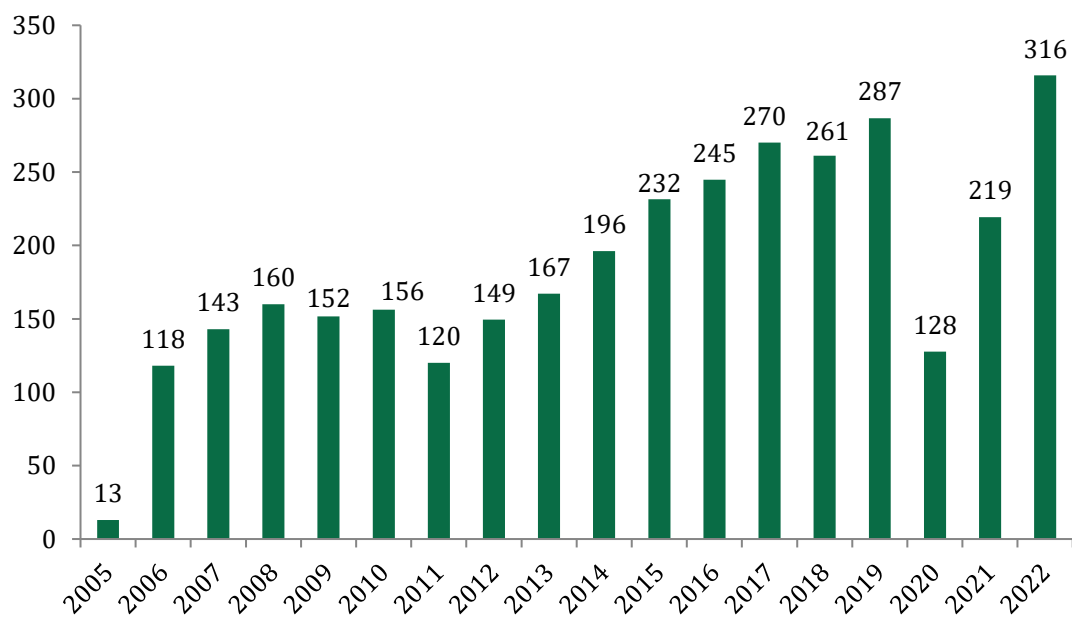


Source : Direction de la sécurité sociale.

Entre 2005 et 2012, les montants de fraudes et activités fautives détectées et stoppées par l'assurance maladie ont été multipliés par 11,5, passant de 13 M€ en 2005 à 149,4 M€ en 2012. Entre 2013 et 2019, ces montants ont connus une forte progression, dépassant les 200 M€ chaque année à partir de 2015.

En 2020 et 2021, la crise sanitaire a conduit à une baisse des montants de fraude détectée et stoppée, accompagnée d'une révision des objectifs annuels.

Graphique 2 : Montant de fraude et activité détectées et stoppées entre 2005 et 2022 (en millions d'euros)



Source : CNAM, mission.

Annexe III

Les **montants des préjudices frauduleux et fautifs (subis et évités) détectés ont progressé au début de la COG⁵ 2018-2022, passant de 261 M€ en 2018 à 287M€ en 2019, puis, compte-tenu de la gestion des effets de la crise sanitaire, ces montants ont connu un fort recul en 2020 (127,7 M€) et 2021 (219,3 M€)**

Depuis 2021, les montants de fraude détectée et stoppée sont à nouveau en hausse et ont atteint **315,8 M€ en 2022**, niveau le plus élevé depuis la mise en place de stratégie de lutte contre la fraude. Ces montants sont composés de 228,7 M€ de préjudice subi et de 87,1 M€ de préjudice évité.

Au sein de la fraude, l'Assurance maladie distingue quatre catégories :

- ◆ obtention des droits ;
- ◆ prestations en espèces ;
- ◆ frais de santé ;
- ◆ établissements.

La principale source de fraude, en montant détecté, concerne les frais de santé (cf. tableau 1), qui représentaient près de la moitié de la fraude en 2018 et 2019 et plus de 68% de la fraude en 2021.

La progression relative de cette catégorie de fraude est principalement liée au recul de la fraude détectée au sein des établissements de santé suite à l'arrêt total des contrôles T2A lors de la crise sanitaire intervenue en 2020 et 2021 (cf. graphique 3). En 2020, 7,9 M€ de fraudes ont été détectés à l'occasion de contrôles T2A et 16 M€ hors T2A (pour un total de 23,9 M€). En 2021, seuls les contrôles hors T2A ont permis de détecter 18 M€ de fraude provenant des établissements de santé.

Tableau 1 : Montant des fraudes et activités fautives détectées et stoppées par la CNAM entre 2017 et 2021, par catégorie (en M€)

Catégorie de fraude	2017	2018	2019	2020	2021
Frais de santé	136,3	128,8	140,1	74,6	149,1
Établissements	91,5	79	89,2	23,9	18
Prestations en espèces	31,3	42,4	44,6	20,5	37
Obtention des droits	10,9	11	12,9	8,7	15,2
TOTAL	270	261,2⁶	286,8	127,7	219,3

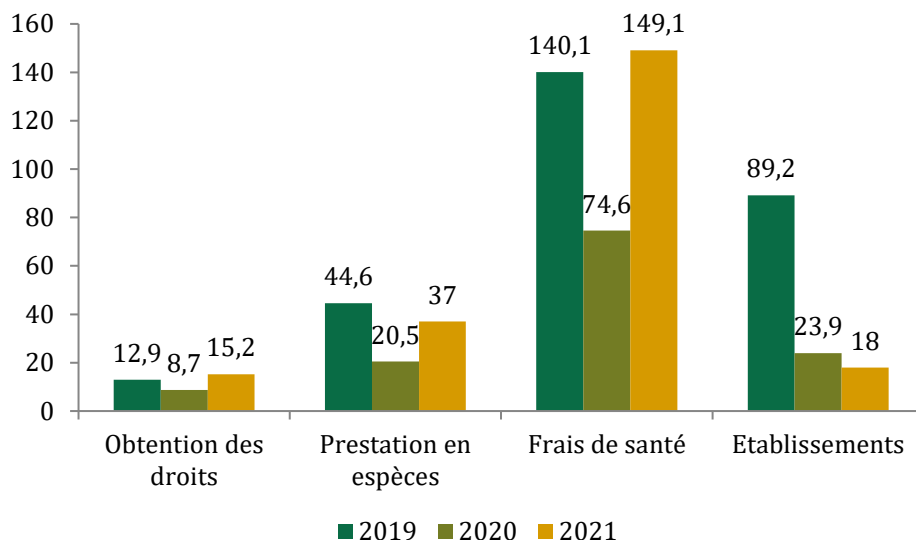
Source : CNAM.

⁵ Cf. 2.1.1

⁶Moratoire contrôles T2A sur les hospitalisations de jour en 2018.

Annexe III

Graphique 3 : Répartition des montants de fraude par catégorie de préjudice financier en 2019 et 2021 (en M€)



Source : CNAM.

Parmi les acteurs à l'origine de la fraude détectée, les **assurés représentaient 68 % des dossiers instruits** en 2021. Au cours de la période 2017-2020, la part des dossiers de fraude concernant des assurés était chaque année supérieure à la moitié des dossiers traités par l'assurance maladie (cf. tableau 2).

Cependant, s'agissant des montants financiers, la part des assurés est bien plus faible et ne représente que 27% du préjudice subi ou évité en 2021. Les préjudices provenant des professionnels de santé et des établissements représentaient plus des trois quarts des montants de fraude détectée et stoppés (cf. tableau 3).

Tableau 2 : Montant des fraudes et activités fautives détectées et stoppées par la CNAM entre 2017 et 2021, en fonction de l'origine de la fraude

Fraudes et activités fautives détectées et stoppées (en M€)	2017	2018	2019	2020	2021
Nombre de dossiers qualifiés de fraudes et d'activités fautives	7 765	22 962	21 292	11 490	12 977
Part des assurés dans les dossiers contrôlés	50%	51%	51%	60%	68%
Montant du préjudice subi ou évité (en M€)	270	261,2	286,7	127,7	219,3
Part des assurés en montant financier	21,3%	22,12%	21%	29%	27%

Source : CNAM, mission.

Concernant les modalités de fraude détectées, **les dossiers instruits par l'assurance maladie se rapportent en premier lieu à des prestations fictives et des facturations multiples ou frauduleuses (34%)** d'une part, et de **non-respect de la nomenclature ou de la réglementation (29%)** d'autre part.

Toutefois, si l'on considère le montant du préjudice, la fraude à la prescription (fausses ordonnances, etc.) représente le premier motif de préjudice financier pour l'assurance, soit 43% des sommes concernées, suivie des actes fictifs (31%).

Annexe III

Tableau 3 : La fraude par acteurs : nombres et montants en 2021

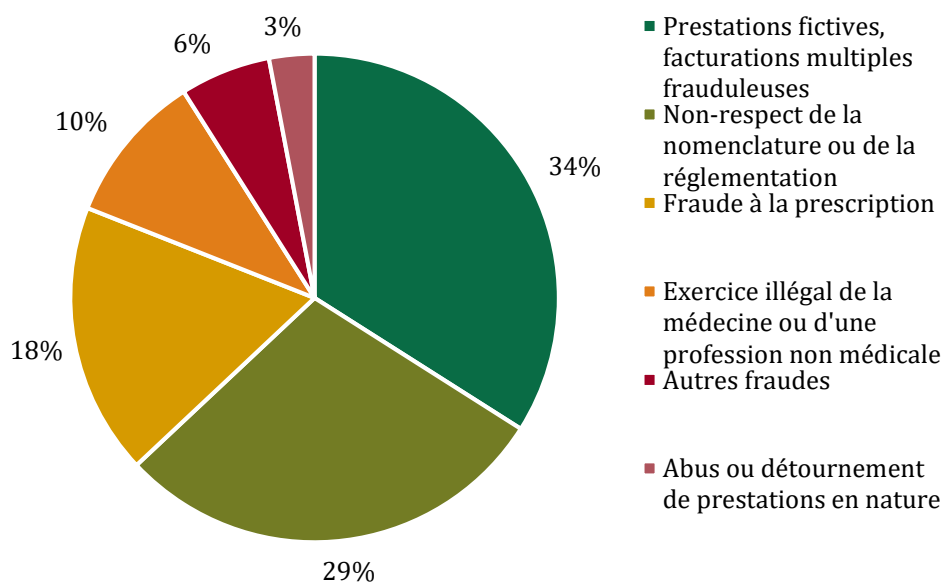
Fraudes détectées et stoppées	Assurés	Offreurs de soins et services	Employeurs	Établissements
En nombre de dossiers	68%	25%	4%	3%
En montant financier	27%	64%	1%	8%

Source : CNAM.

À titre d'exemple, l'étude des données relatives aux **médecins généralistes** fait apparaître que :

- ◆ les **prestations fictives et les facturations multiples et frauduleuses** constituaient **en 2021, plus du tiers des dossiers** de fraude détecté, et 31% du préjudice financier rattaché à cette profession (cf. graphique 4 et graphique 5) ;
- ◆ **la fraude à la prescription**, qui comptait pour 18% des dossiers de fraude, représentait quant à elle **43% des montants de fraude identifiée**.

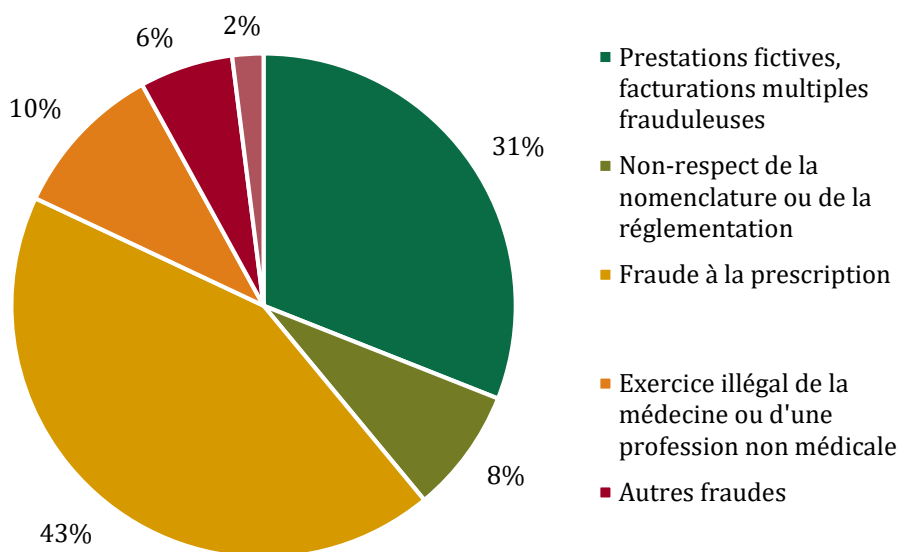
Graphique 4 : Répartition du nombre de dossiers détecté en 2021 par type de fraude pour les médecins généralistes (en %)



Source : CNAM.

Annexe III

Graphique 5 : Répartition du préjudice financier détecté en 2021 par type de fraude pour les médecins généralistes (en %)



Source : CNAM.

Tableau 4 : Montant des préjudices détectés et stoppés causés par les professionnels de santé, en frais de santé par profession entre 2016 et 2021 (en M€)

Profession	2016	2017	2018	2019	2020	2021
Infirmiers	31,8	31,2	34	39	17	39
Pharmaciens	14	14,6	12,3	18	9	19
Prestataires de service et fournisseurs de matériels ⁷	7	8,3	8,7	7	2	16
Chirurgiens-plasticiens	NC	NC	NC	15	13	14
Transporteurs	14,7	19,1	16,3	21	6	14
Médecins spécialistes	7	5,8	4,5	9	5	14
Masseurs-kinésithérapeutes	5,16	5,2	6	9	3	8
Médecins généralistes	4,9	5,3	4	9	5	6
Chirurgiens-dentistes	2,2	1,9	1,5	4	1,5	3
Laboratoires	0,3	0,6	0,6	2	1	2
Total	87,1	92	88,3	133	62,5	121

Source : CNAM.

En montants détectés, la fraude des assurés est principalement (cf. tableau 5) une fraude aux indemnités journalières (21,2 % du total en 2021) et une fraude aux rentes suite à un accident du travail (29,5 % du total en 2021).

⁷ Pour 2016 et 2017 les données sont celles de la catégorie "Fournisseurs" ajoutées à celles d'"Autres prestataires de service", issues du bilan de lutte contre la fraude de la CNAM.

Annexe III

Tableau 5 : Fraude des assurés détectée et stoppée par l'assurance maladie en 2021, par types de griefs

Griefs	Fraudes ayant donné lieu à action		Préjudice (subi et évité)	
	Nombre d'acteurs	Part (en %)	Montant total (en M€)	Part (en %)
Abus ou détournement de prestations en nature	48	0,5%	0,2	0,3%
Autres fraudes	87	0,9%	1,8	3,0%
Cumul IJ, non-respect des règles de sortie ou autres fraudes aux IJ	1 665	17,9%	12,6	21,2%
Factures falsifiées, surchargées, contrefaites	64	0,7%	0,3	0,5%
Falsification d'arrêt de travail ou pièces justificatives	845	9,1%	2,8	4,7%
Falsification ou non-respect des règles de facturation prévues par la LPP	15	0,2%	0,2	0,3%
Fraude à la prescription	271	2,9%	1,3	2,2%
Fraude à l'ASI	296	3,2%	2,4	4,0%
Fraude à la reconnaissance et au maintien- rentes AT	664	7,1%	17,5	29,5%
Fraudes à la condition de résidence - AME	98	1,1%	0,7	1,2%
Fraudes aux conditions de ressources et de résidence -C2S/CMUC/ACS	2 798	30,1%	3,9	6,6%
Fraudes aux conditions de ressources et de résidence -PUMa	1 365	14,7%	9	15,2%
Fraude travailleurs frontaliers	110	1,2%	0,5	0,8%
Médicaments abus et trafics	784	8,4%	5,2	8,8%
Non déclaration d'un changement dans la situation	178	1,9%	0,7	1,2%
Prestations fictives, facturations multiples frauduleuses	10	0,1%	0,1	0,2%
Total 2021	9 298	100 %	59,3	100 %
<i>Total 2020</i>	<i>5885</i>	-	<i>36,3</i>	-
<i>Total 2019</i>	<i>10 439</i>	-	<i>56,1</i>	-

Source : CNAM.

1.2. Les premiers travaux d'estimation de la fraude lancés en 2020 sont encore incomplets mais font apparaître un niveau de fraude entre cinq et vingt fois supérieur à la fraude détectée selon les professions de santé

Comme l'a relevé la Cour des comptes dans son rapport de septembre 2020 relatif à la lutte contre la fraude sociale, les chiffres de fraude détectée et évitée donnent une **vision potentiellement sous-estimée et partielle au regard du montant total des prestations versées**, en l'absence d'estimation ex ante de la fraude en question.

En effet, il est important de signaler que **la progression des montants de fraude détectés par l'Assurance maladie au cours des dernières années ne donne pas d'information sur l'éventuelle progression de la fraude elle-même** mais renseigne sur l'amélioration de l'efficacité des actions entreprises par l'Assurance maladie.

À la suite du rapport de la Cour de comptes et de celui établi par la commission d'enquête parlementaire relative à la lutte contre les fraudes aux prestations sociales, présidée par M. Patrick Hetzel⁸, **la CNAM a engagé à partir de novembre 2020 un travail d'évaluation du montant des fraudes** commises par les établissements, les professionnels et les assurés.

Par ailleurs, une **feuille de route du 9 décembre 2020** a été co-signée par trois ministères⁹ et transmise à la direction de la sécurité sociale. Cette feuille de route fait de la cartographie de la lutte contre les fraudes sociales un axe de travail, le DSS étant chargé de solliciter des caisses nationales de sécurité sociale une estimation chiffrée et mise à jour de façon biennale des fraudes dont elles peuvent être victimes.

En janvier 2021, un plan d'action de lutte contre les fraudes sociales pour 2021 et 2022, élaboré avec toutes les caisses nationales d'assurance maladie, a ensuite été validé en COPIL fraudes avec le ministère des comptes publics.

1.2.1. La CNAM a fait le choix de méthodes statistiques éprouvées par d'autres organismes de sécurité sociale et par les administrations afin d'évaluer l'ampleur de la fraude

1.2.1.1. Depuis 2020, des échanges nombreux avec d'autres organismes publics confrontés à la fraude, en France et en Europe

Lors du lancement des travaux d'évaluation d'ampleur de la fraude à l'assurance maladie, la CNAM a décidé de ne pas recourir à la constitution d'échantillons représentatifs. Selon cette dernière, la méthode ne convient pas aux spécificités de l'activité de l'assurance maladie qui compte « *trop de variété de professions, de nombre d'actes et aurait constitué une perte de temps et de moyens* », en employant trop largement les ressources rares que sont les praticiens-conseil et les agents habilités et agréés à opérer des contrôles¹⁰.

La CNAM a d'abord réalisé un travail de **comparaison des méthodes d'estimation de la fraude employées en France** (par les autres branches du régime général et les autres régimes, Pôle Emploi, la CCMSA, l'INSEE) **et en Europe** (notamment en Allemagne et Angleterre) de janvier à avril 2021. L'objectif était d'identifier les principales méthodes statistiques d'évaluation de la fraude déjà utilisées, et de disposer de retours d'expériences sur les avantages et contraintes de chacune des méthodes retenues.

⁸ Rapport n° 3300 de l'Assemblée nationale, en date du 8 septembre 2020, fait au nom de la commission d'enquête relative à la lutte contre les fraudes aux prestations sociales,

⁹ Ministère des solidarités et de la santé, ministère des comptes publics, ministère du travail.

¹⁰ Article L. 161-29 du code de la sécurité sociale

Encadré 1 : Comparaisons internationales et recherche de bonnes pratiques dans d'autres pays européens

La CNAM a mené, à partir de 2020, des échanges avec divers homologues européens pour identifier les méthodes d'évaluation de la fraude retenue à l'étranger :

- échanges avec le **Royaume-Uni** (National Health Service – Counter Fraud Authority). Le NHS-CFA est une structure créée en 2017 et rattachée au NHS. Elle est chargée de la lutte contre la fraude et de son évaluation. Celle-ci se fait sur la base d'un **questionnaire envoyé aux assurés ayant eu recours à un professionnel de santé et par tirage aléatoire**. Les professionnels de santé étant des salariés de la NHS, leur fraude est considérée comme de la fraude interne ;
- échanges avec **l'Allemagne (Gesetzliche Krankenversicherung -GKV)**, organisme public d'Assurance Maladie allemand, qui ne dispose pas de méthode identifiée, et se trouve également en phase de recherche pour procéder à l'évaluation des préjudices liées à la fraude ;
- **webinaires sur l'évaluation de la fraude, à l'initiative de la CNAM et de l'INAMI (Institut national d'assurance maladie-invalidité, Belgique) avec l'EHFCN (European Healthcare Fraud & Corruption Network)** qui rassemble des organismes d'assurance en santé sur le sujet de la fraude, au cours du dernier trimestre 2020. Ce sujet n'est pas d'actualité dans les pays présents dans le cadre de l'EHFCN. Ces rencontres ont eu pour objectif de partager des expériences et des expertises sur plusieurs thématiques dont l'évaluation chiffrée de la fraude.

Source : CNAM.

Parmi les contacts pris par la CNAM, ceux auprès de l'URSSAF Caisse nationale ou de la MSA ont permis de mettre en exergue **l'intérêt à court terme du recours aux méthodes de post stratification ou économétrique, sur la base des résultats des contrôles déjà réalisés**, pour estimer le préjudice financier. Ces méthodes ont été utilisées pour les premiers risques cartographiés.

Quelle que soit la méthode utilisée, les organismes rencontrés, qui disposent d'un chiffrage de la fraude, ont en commun un **investissement dans le temps pour affiner la méthodologie retenue sur un périmètre progressif étalé sur plusieurs années** :

- ◆ **l'URSSAF (caisse nationale)** a utilisé les **méthodes d'estimation par post-stratification et par contrôles aléatoires**. Ce type de méthode a par exemple été appliqué sur les données URSSAF de l'agglomération lyonnaise pour l'estimation du manque à gagner issu des contrôles comptables d'assiette¹¹. La méthodologie mise en place pour évaluer la fraude globale tient compte du problème de sélection et de non-détection en incorporant explicitement un processus de détection dans le modèle de fraude et en permettant une variation dans les taux de détection ;
- ◆ **la MSA**, dont l'engagement n°27 de la COG 2016-2020 fixait une échéance de livrable d'une étude d'évaluation de la fraude pour 2019, a produit une première estimation du manque à gagner sur des données de 2011 en mettant également en œuvre la **méthode d'extrapolation par post-stratification**. Dans un second temps, le choix a été fait d'utiliser la **méthode économétrique sur le domaine du recouvrement des cotisations**, méthode jugée plus fiable et sollicitant peu le réseau des caisses.

La CNAM a également conduit des échanges avec **l'INSEE qui mène, en lien avec la Direction générale des finances publiques (DGFIP), des travaux sur l'évaluation de la fraude fiscale**, et notamment l'estimation des montants manquants de versements de TVA. Les travaux ont permis d'identifier l'usage de **techniques relatives à la définition de plan de sondage et à l'application de la méthode de détermination de la « probabilité d'inclusion »**, deux techniques qui peuvent constituer des perspectives à moyen terme.

¹¹ Nadia Joubert, Processus de détection et évaluation de la fraude sociale, Revue économique, volume 60, 2009.

1.2.1.2. *Le choix de méthodes statistiques pertinentes au regard de l'activité de l'assurance maladie*

Depuis 2020, les travaux d'évaluation de l'ampleur de la fraude se sont appuyés sur plusieurs méthodes, afin d'en vérifier la pertinence, tant pour les résultats obtenus que pour les moyens à mettre en œuvre pour y parvenir. A l'issue des premières campagnes d'évaluation, la méthode statistique dite de *matching* a été retenue à titre principal.

L'extrapolation à partir de contrôles réalisés sur la base d'un tirage aléatoire s'appuie sur un échantillon représentatif de la population étudiée. En ce sens, elle ne fait donc l'objet d'aucun biais de sélection (au sens où l'estimation du préjudice n'est pas basée sur les seuls contrôles ciblés). En revanche, elle implique une forte mobilisation de moyens humains pour effectuer des contrôles, alors que la priorité est donnée au sein de l'Assurance Maladie aux contrôles ciblés dans une logique d'efficience.

Afin de produire ses estimations de l'ampleur de la fraude, l'Assurance Maladie dispose d'ores et déjà de **deux sources de données provenant des contrôles réalisés depuis plusieurs années**:

- ◆ la première source provient des **résultats des actions de contrôles-contentieux** conduits par les services lutte contre la fraude des caisses primaires d'assurance maladie (CPAM) en lien avec les directions régionales du service médical :
 - cette stratégie de contrôle contentieux s'appuie sur des **programmes nationaux et locaux**. À titre d'illustration, en 2019, avant la crise sanitaire de 2020, 29 programmes nationaux et 17 programmes d'actions régionaux ont été lancés et déployés sur le territoire ;
 - le choix de ces programmes nationaux de contrôle-contentieux, pilotés jusqu'en 2022 par la Direction de l'Audit, du Contrôle-Contentieux et de la Répression de la Fraude (DACC RF)¹² de la CNAM s'appuie sur divers éléments, tels que :
 - l'évolution des dépenses remboursées par l'Assurance maladie ;
 - les cartographies des risques de fraudes ;
 - l'analyse des résultats des programmes nationaux antérieurs.
 - **l'ensemble des résultats des contrôles-contentieux est retracé dans une base unique de données OG3S** (outil de gestion des signalements et de suivi des suites contentieuses), qui permet de réaliser annuellement le bilan de la politique de lutte contre la fraude et les activités fautives, tel que prévu par l'article L 1149 du code de la sécurité sociale.
- ◆ **la seconde source renvoie aux campagnes annuelles de contrôles des paiements** organisée par la Direction Déléguée des Finances et de la Comptabilité (DDFC) en lien avec les CPAM. Il s'agit des contrôles ciblés sur quatre catégories de professionnels de santé :
 - infirmiers libéraux (IDEL) ;
 - transporteurs sanitaires ;
 - pharmaciens ;
 - masseurs-kinésithérapeutes.

¹² Intégrée désormais à la DDAFF.

Annexe III

Ces contrôles aléatoires visent à rechercher des atypies de facturation et à mesurer le risque résiduel au détriment d'un bénéficiaire, que ce soit l'Assurance Maladie, un assuré ou un professionnel de santé. Le tirage des factures à contrôler se fait selon les montants remboursés les plus élevés avec, au total, **125 000 factures par catégorie de professionnels de santé à contrôler par an sur l'ensemble du réseau**. Ces contrôles répondent à une même logique de ciblage que ceux effectués dans le cadre des programmes nationaux ou régionaux de lutte contre la fraude, notamment quant aux montants remboursés importants. Leur intégration dans le périmètre des données étudiées pour l'évaluation permet en outre un **volume plus approprié à une meilleure modélisation des données, en prenant en compte une base large de professionnels de santé contrôlés**.

Toutefois, compte-tenu de la diversité des prestations versées, de la multitude d'acteurs, et des règles de facturation propres à chaque acteur, la CNAM a retenu les méthodes d'extrapolation statistiques, en s'appuyant sur les travaux d'un cabinet spécialisé¹³, afin d'établir une **estimation par type de prestations sur la base du calcul d'un taux de préjudice financier pour chacune d'entre elles**.

La méthode d'extrapolation par post-stratification issue des contrôles ciblés consiste, dans un premier temps, à stratifier la population contrôlée selon des critères jugés pertinents dans le ciblage des acteurs. Puis il s'agit d'effectuer une extrapolation des résultats pour chaque strate et de les agréger en les pondérant par leur poids dans la population totale étudiée.

Cette méthode ne corrige, en revanche, que partiellement le biais de sélection car le nombre de critères de post-stratification est contraint, chaque strate devant disposer d'un volume de données suffisant pour rendre l'estimation robuste. En outre, elle ne corrige pas du biais de détection des fautes ou fraudes.

À titre d'exemple, une évaluation du manque à gagner en matière de cotisations sociales dans le secteur privé réalisée en 2012 s'était appuyée sur la méthode de post-stratification. Les résultats avaient conduit à relever sensiblement l'estimation du niveau de fraude aux cotisations sociales par rapport à la méthode des contrôles aléatoires :

- ◆ entre 4,5 et 7,4 Mds€ avec la méthode de contrôles aléatoires ;
- ◆ entre 16,3 et 26,9 Mds€ avec la méthode de post-stratification¹⁴.

La méthode économétrique est également appliquée aux contrôles ciblés. Elle consiste à estimer les comportements de fraude à partir d'un modèle qui intègre le processus de sélection comme indiqué par le conseil national de l'information statistique (CNIS)¹⁵. Ainsi, cette méthode permet de s'affranchir du biais de sélection. Elle peut également corriger du biais de non-détection dont ne tient pas compte l'extrapolation par post-stratification.

Dans le cadre des premiers travaux d'évaluation de la fraude des **infirmiers libéraux (IDEL)**, la CNAM a appliqué la **méthode économétrique** (méthode d'Heckman), en s'inspirant des travaux réalisés par la MSA pour déterminer la variable instrumentale du modèle. La MSA avait retenu les effectifs dédiés à la lutte contre la fraude comme variable instrumentale du contrôle. Cet instrument s'est cependant avéré « fragile », selon la CNAM, cette variable étant très faiblement explicative du contrôle puisque les ETP d'un service de lutte contre la fraude d'une CPAM sont affectés au contrôle de l'ensemble des professions de santé (un investigateur peut porter son effort sur les IDE autant que sur les pharmacies par exemple). La taille des équipes dédiées à la lutte contre la fraude a également un impact sur la variété de professions de santé qui font l'objet d'un contrôle, ce qui peut paradoxalement réduire la part des professionnels contrôlés pour chacune des professions considérées isolément.

¹³ K Stat Consulting

¹⁴ « La mesure du travail dissimulé et ses impacts pour les finances publiques, rapport du groupe de travail du Cnis », CNIS, juin 2017

¹⁵ Ibid.

Annexe III

Pour la suite des évaluations, **la méthode d'Heckman a été abandonnée au profit de la méthode d'appariement, dite de « matching »**, notamment au regard de la difficulté de trouver une variable d'exclusion satisfaisante, permettant d'expliquer le contrôle sans influencer directement sur la fraude, au risque sinon de rencontrer un problème de colinéarité.

Tableau 6 : Panorama des méthodes statistiques employées par la CNAM

Description	Méthode économétrique	Méthode de « matching »	Méthode de post-stratification
Objectif	Estimer conjointement la probabilité de contrôle et de fraude de chaque individu puis le montant de fraude corrigé des biais de sélection.	Apparier les médecins non-contrôlés aux médecins contrôlés avec des caractéristiques semblables. Chaque médecin non-contrôlé est apparié aux médecins contrôlés dont la probabilité de fraude se situe dans un intervalle défini.	Stratifier a posteriori la population des médecins selon des critères jugés pertinents dans le ciblage des acteurs.
Modalités de calcul	Agrégation des résultats en sommant pour l'ensemble des acteurs l'espérance de fraude estimée	Extrapolation des résultats, par règle de trois, pour chaque médecin non-contrôlé en utilisant le taux de préjudice financier moyen sur les médecins contrôlés appariés	Extrapolation des résultats, par règle de trois, pour chaque strate en utilisant le taux de préjudice financier moyen sur les médecins contrôlés. Agrégation des résultats en les pondérant par leur poids dans la population totale étudiée
Limites	Cette méthode a l'avantage de mieux corriger du biais de sélection à condition que les critères de contrôle et de fraude soient observables. Toutefois, les variables observables doivent être explicatives du contrôle, de la fraude et du montant de fraude. Le processus de sélection doit être connu et stable entre les années	Cette méthode ne corrige que partiellement les biais de sélection. Le processus de sélection ne doit s'appuyer que sur les variables observées. Des individus aux caractéristiques similaires doivent pouvoir être contrôlés ou non pour pouvoir réaliser l'appariement	Cette méthode ne corrige que partiellement du biais de sélection car le nombre de critères de post-stratification est contraint au fait que chaque strate doit disposer d'un volume de données suffisant pour rendre l'estimation robuste (à minima 30 médecins contrôlés par strate)

Source : CNAM.

1.2.2. Des résultats partiels qui font apparaître un niveau de fraude élevé au sein des professions de santé examinées, entre 5% et 7% chez les infirmiers libéraux

Les résultats des premières estimations relatives à la fraude de la part des bénéficiaires de la C2S et des infirmiers ont été communiqués à la fin de l'année 2021.

S'agissant de la **fraude aux soins infirmiers**, les travaux ont porté sur les résultats des actions de contrôle et de lutte contre la fraude mettant en exergue les préjudices financiers sur l'année 2018. Deux méthodes statistiques ont été utilisées :

- ◆ une méthode post stratification qui aboutit à un taux de préjudice financier de 5 % (286 M€) ;
- ◆ une méthode économétrique qui aboutit à un taux de préjudice financier de 6,9% (393 M€).

Annexe III

L'évaluation de la fraude à la complémentaire santé solidaire (C2S) a été effectuée à partir de 10 700 dossiers tirés aléatoirement en 2018 et 2019. Le montant du préjudice financier global est estimé entre 25 M€ et 176,5 M€ par an en fonction des méthodologies appliquées. Deux méthodes ont été appliquées :

- ◆ le pourcentage de dossiers pour lesquels les ressources réellement perçues sont supérieures à trois fois les plafonds ;
- ◆ le pourcentage de dossiers pour lesquels les ressources réellement perçues dépassent les plafonds.

Dans le cadre de sa stratégie "globale renouvelée" de lutte contre la fraude, présentée le 30 septembre 2022, la CNAM a dévoilé les résultats de ses travaux d'évaluation du risque de fraude pour les **médecins généralistes**¹⁶. Le préjudice est estimé **entre 3,1% et 3,5% des dépenses**, soit de 185 à 285 millions d'euros par an.

Pour les 57 000 généralistes, les travaux font apparaître une estimation du préjudice financier comprise entre 3,1% (en 2018) et 3,5% des dépenses (en 2019). Soit 185 à 215 millions d'euros, sur un total de 6 milliards. Un chiffre à mettre en regard du montant du préjudice financier des fraudes réellement détectées en 2019, 9 millions d'euros.

Tableau 7 : Montants estimés de fraude obtenus au moyen de méthodes statistiques, par catégorie professionnelle (données 2019)

Profession de santé contrôlée	Montants totaux remboursés (en M€)	Montants préjudices financiers détectés (en M€)	Taux de préjudice financier détecté (%)	Extrapolation brute		Extrapolation statistique	
				Montants préjudices extrapolés (en M€)	Taux de préjudice financier	Montants préjudices extrapolés	Taux de préjudice financier
Infirmiers libéraux (IDEL)*	5 700	17,8	0,3%	339	5,9%	286	5%
Médecins généralistes	6 200	3,7	0,1%	252	4,0%	215	3,5%
Transporteurs	3 700	6,9	0,2%	163	4,4%	145	3,9%
Pharmaciens	19 200	7,9	0,0%	155	0,8%	91	0,5%
Masseurs-kinésithérapeutes	3 500	4,3	0,1%	261	7,60%	234	6,80%

*Source : CNAM, mission. *Pour les infirmiers libéraux, données 2018.*

En 2023, la CNAM prévoit le lancement de nouvelles évaluations afin de couvrir la quasi-totalité des segments de son activité :

- ◆ au **premier semestre**, les évaluations concerneront :
 - les chirurgiens-dentistes ;
 - les rentes accident du travail-maladie professionnelle ;
 - la protection universelle maladie (PUMa) ;
- ◆ au **second semestre**, les évaluations porteront sur :
 - les médecins spécialistes ;
 - les pensions d'invalidité ;
 - les laboratoires ;
 - les fournisseurs de produits inscrits sur la liste des produits et prestations (LPP) ;
 - les services de soins infirmiers à domicile (SSIAD).

¹⁶ Exerçant en ville.

Annexe III

Ces **premières estimations confirment la prise en compte insuffisante des risques de fraudes dans la conception actuelle des dispositifs de contrôle interne et de lutte contre les fraudes**, notamment le nombre globalement insuffisant des contrôles de toute nature au regard d'indices convergents d'anomalies.

Jusqu'à présent, la démarche d'évaluation de l'ampleur de la fraude s'est concrétisée sur un champ partiel des dépenses de l'assurance maladie. La poursuite de ces efforts permettra à moyen terme à la CNAM de mieux orienter ses efforts de prévention et de détection des fraudes en fonction des enjeux.

Annexe III

Tableau 8 : Évaluation de l'ampleur de la fraude, méthodes statistiques (données 2018 et 2019)

Profession de santé contrôlée	Années de référence	Date de l'évaluation	Nombre de professionnels pris en compte	Montants totaux remboursés (en M€)	Montants totaux contrôlés (en M€)	Montants préjudices financiers (en M€)	Taux de préjudice financier détecté (%)	Extrapolation brute		Extrapolation statistique (post-stratification ou matching)	
								Montants préjudices financiers extrapolés (en M€)	Taux de préjudice financier	Montants préjudices financiers extrapolés (en M€)	Taux de préjudice financier
Infirmiers libéraux (IDEL)	2018	Septembre 2021	91 000	5 700	300,8	17,8	0,3%	339	5,9%	286	5%
	2019	Septembre 2022	91 000	5 700	300,8	17,8	0,3%	339	5,9%	286	5%
Médecins généralistes	2018	Juillet 2022	57 000	6 000	95	4	0,1%	256	4,3%	185	3,1%
	2019		56 000	6 200	91	3,7	0,1%	252	4,0%	215	3,5%
Transporteurs	2018	Septembre 2022	30 000	3 600	327	12,3	0,3%	182	5,1%	177	4,9%
	2019		29 000	3 700	216	6,9	0,2%	163	4,4%	145	3,9%
Pharmaciens	2018	Novembre 2022	20 000	17 500	1 300	11,3	0,1%	151	0,9%	105	0,6%
	2019		20 000	19 200	936	7,9	0,0%	155	0,8%	91	0,5%
Masseurs-kinésithérapeutes	2018	Décembre 2022	64 000	3 200	61,7	4,7	0,1%	245	7,6%	166	5,2%
	2019		66 000	3 500	56,2	4,3	0,1%	261	7,6%	234	6,8%

Source : CNAM.

1.3. La fraude des assurés et des professionnels de santé peut impliquer l'utilisation de la carte Vitale sans toutefois que ne soit identifiée par l'Assurance maladie une fraude de grande ampleur spécifique à ce support

1.3.1. La définition de la fraude par l'Assurance maladie inclut les détournements d'usage de la carte Vitale mais ce grief ne représente que 24 dossiers depuis 2018 pour un préjudice total cumulé inférieur à 45 000€

La fraude à l'Assurance maladie est diversifiée sur le plan des acteurs (professionnels de santé libéraux, établissements de santé, assurés, employeurs) et des modalités (facturations d'actes médicaux et paramédicaux, séjours en établissements de santé, prestations et bien de santé fictifs, fausses facturations...).

La fraude est définie par la CNAM comme établie pour « *les faits illicites au regard des textes juridiques¹⁷, commis intentionnellement par une ou plusieurs personnes physiques ou morales (assuré, employeur, professionnel de santé, fournisseur, transporteur, établissement, autre prestataire de services, employé de l'organisme) dans le but d'obtenir ou de faire obtenir un avantage ou le bénéfice d'une prestation injustifiée ou indue au préjudice d'un organisme d'assurance maladie ou de la caisse d'assurance retraite et santé au travail ou encore de l'État s'agissant de la protection complémentaire en matière de santé, du bénéfice de l'aide au paiement d'une assurance complémentaire de santé ou de l'aide médicale de l'État* ». ¹⁸

Dans l'ensemble des actions frauduleuses, une graduation est constatée par les services de la CNAM qui prennent en compte des pratiques fautives d'une part, et des pratiques abusives d'autre part :

- ♦ **les fautes** sont les activités qui « rassemblent de manière réitérée des faits irréguliers au regard de textes juridiques (notamment les nomenclatures), commis par une ou plusieurs personnes physiques ou morales en dehors des circonstances définissant la fraude ou les activités abusives. Les fautes peuvent être constatées en cas d'**absence d'information d'un changement de situation familiale impactant les droits** ; de **non-respect des règles de facturation** par les professionnels de santé ou établissements de santé (dépassements du nombre d'actes facturables par jour, de cotations erronées, de majorations non prévues par la nomenclature) »¹⁹ ;
- ♦ **les pratiques abusives** sont celles qui « rassemblent de manière réitérée des faits caractéristiques d'une utilisation d'un bien, d'un service ou d'une prérogative **outrepassant des niveaux acceptables par rapport à des références ou des comparatifs non juridiques**, notamment l'exécution d'actes médicaux allant au-delà du besoin de soins du patient ».

La CNAM assure le suivi des différents griefs caractérisant la fraude aux prestations dont elle assure le remboursement. Ce suivi est retracé dans son **bilan annuel de lutte contre la fraude et les activités fautives** établi conformément à l'article L. 1149 du code de la Sécurité sociale.

Parmi les griefs qui font l'objet d'un suivi par la CNAM, figurent les « **détournements de l'usage de la Carte Vitale** ». Toutefois, pour la période allant de 2018 à 2022, les montants de fraude rattachables à ce grief s'avèrent très faibles : moins de dix dossiers par an, pour des montants annuels inférieurs à 60 000 € (cf. tableau 9).

¹⁷ Une fraude ne peut être qualifiée en tant que telle que si l'infraction correspondante est expressément prévue par un texte juridique, notamment les articles 441-1 et 313-1 du code pénal.

¹⁸ Circulaire CNAM CIR-1/2012, en date du 2 janvier 2012.

¹⁹ Circulaire CNAM CIR-1/2012, en date du 2 janvier 2012.

Annexe III

Il convient de noter que les fraudes détectées ne font pas apparaître l'usage de cartes Vitale contrefaites. Dans les cas de fraude détectée, ce sont donc de véritables cartes Vitale produites par le GIE SESAM-Vitale qui font l'objet d'un détournement d'usage, et non des contrefaçons.

Tableau 9 : Montant des griefs relatifs au « détournement de la carte Vitale » détectés par la CNAM entre 2018 et 2022

Exercice	Nombre de dossiers	Préjudice financier total (en €)	Préjudice financier moyen (en €)
2018	6	47 587	7 931
2019	2	53 653	26 827
2020	3	58 772	19 591
2021	4	3 725	931
2022	9	44 971	4 997
Total cumulé 2018-2022	24	208 708	8 696

Source : CNAM.

1.3.2. La carte Vitale peut constituer un mode opératoire dans d'autres types de fraudes, commises par des assurés et des professionnels de santé, en premier lieu les facturations d'actes fictifs

Toutefois, l'utilisation irrégulière de la carte Vitale constitue principalement un mode opératoire dans le cadre de différents types fraudes et non un grief à part entière. Ainsi, en complément du grief « détournement de la carte Vitale » évoqué précédemment, plusieurs autres griefs définis par la CNAM sont susceptibles d'impliquer une utilisation frauduleuse de la carte Vitale (cf. Tableau 10), notamment :

- ◆ la facturation d'actes fictifs ;
- ◆ la fraude à l'identité ;
- ◆ le trafic de médicaments ;
- ◆ l'usurpation de droits.

Le périmètre de ces griefs est plus large que la seule « fraude à la carte vitale », en particulier pour 2022 : le montant très élevé des **fraudes liées à des actes fictifs** (84,7 M€, contre 33,7 M€ en 2021) s'explique par des fraudes d'ampleur en lien avec la délivrance fictive de tests antigéniques aux professionnels de santé par des pharmacies.

Ainsi, la fraude liée à la carte Vitale n'est pas identifiée par la CNAM comme un élément majeur de fraude, et aucun plan de lutte contre une « fraude-type » à la carte Vitale n'a été établi, en l'absence de pertinence d'une telle définition.

Tableau 10 : Montant des griefs dont le mode opératoire est lié à une utilisation frauduleuse de la carte Vitale détectés par la CNAM entre 2018 et 2022 (en €)

Griefs	2018	2019	2020	2021	2022
Facturations d'actes fictifs (acte facturé mais non réalisé, double facturation)	23 701 834	30 992 812	18 224 257	33 746 092	84 688 400
Facturations multiples	7 861 299	6 922 518	1 837 088	4 418 516	4 528 460
Fraudes à l'identité	535 158	2 396 698	1 474 646	2 475 307	3 154 027
Trafics de médicament	1 281 194	1 383 376	674 200	1 034 081	1 193 389
Usurpations de droits	368 369	430 808	165 039	308 966	185 646

Source : CNAM.

En distinguant les **modalités de fraude en fonction des acteurs** à l'origine de celle-ci, il est possible d'établir les cas de fraude suivant, impliquant le recours à la carte Vitale :

Annexe III

- ◆ concernant les **bénéficiaires des prestations (assurés ou non-assurés)**, les fraudes à la carte Vitale peuvent comprendre :
 - le détournement de prestations par usurpation de l'identité :
 - au bénéficiaire d'une personne qui **ne justifie pas d'un séjour régulier** lui permettant d'être éligible à la protection universelle maladie (PUMA), associant le cas échéant la carte Vitale à d'autres documents d'identité (« pack »²⁰) ;
 - au bénéficiaire d'une personne qui **ne justifie pas d'un séjour irrégulier lui permettant d'être éligible à l'aide médicale d'État (AME)**, à savoir une durée de résidence de plus de trois mois et l'absence de titre de séjour depuis plus de trois mois, ainsi que des ressources inférieures à un plafond réglementaire. Cette fraude peut associer le cas échéant la carte Vitale à d'autres documents d'identité (« pack ») ;
 - **l'accès au tiers-payant** par usurpation de l'identité d'un assuré bénéficiant d'une affection longue durée (ALD) ou éligible à la complémentaire santé solidaire (C2S), et autres remboursements liés au niveau de ressources ;
 - le **maintien de l'accès aux soins** malgré le non-respect de la condition de **résidence stable en France** par des personnes ayant déjà bénéficié de la PUMA à bon droit (absence de mise à jour des informations à l'origine de l'ouverture de droits) ;
 - la recherche de l'anonymat par usurpation d'identité sans que cela implique que le patient ne soit pas assuré par ailleurs (par exemple dans le cas de grossesses non désirées, de maladies sexuellement transmissibles,...) ;
 - **le bénéfice de certains avantages liés à certaines affections** : ainsi, certaines personnes atteintes par le COVID-19 ont pu pratiquer des tests en utilisant la carte Vitale d'une autre personne afin que cette dernière bénéficie du passe accordé pour quatre mois en cas d'infection et ne soit pas contrainte à se vacciner. Le même procédé peut être mis en œuvre par exemple avec le VIH afin de maintenir un titre de séjour pour soins ;
 - la **délivrance de médicaments** (stupéfiants, onéreux) par l'usage d'une carte Vitale valide associée à une prescription frauduleuse pour la délivrance de médicaments (stupéfiants, onéreux).
- ◆ S'agissant des **professionnels de santé**, ils peuvent utiliser la carte Vitale de l'un de leurs patients et, **même en l'absence de cette carte**, les données de la carte stockées dans le logiciel de facturation pour :
 - facturer des actes fictifs ;
 - facturer des actes plus coûteux que ceux effectivement réalisés (cotation) ;
 - facturer des actes non nécessaires.

Ces fraudes de professionnels de santé peuvent, le cas échéant, être commises avec la complicité de l'assuré.

Le fait que la carte Vitale contienne les données biométriques du patient n'aurait pas d'impact sur certains types d'agissement et ne permettrait pas de les empêcher lorsque le professionnel de santé est à l'initiative de la démarche frauduleuse (cf. Tableau 11).

²⁰ Des packs de documents officiels volés, récupérés à la suite d'une perte ou falsifiés, pouvant associer une carte Vitale à une carte d'identité par exemple, sont vendus sur le dark net.

Tableau 11 : Utilité de l'usage de la biométrie dans la lutte contre les fraudes liées à l'usage de la carte Vitale

Types de fraude	Modalité de la fraude	Portée de la fraude	Efficacité de la carte Vitale biométrique	Commentaire sur l'utilité de la biométrie
Usurpation d'identité (assurés)	Utilisation d'une carte Vitale perdue ou volée	Accès aux prestations de santé (soins, médicaments)	Moyenne	Utilité limitée car les cartes actuelles sont déjà désactivées après le premier usage suivant une déclaration de vol ou de perte
	Fraude au tiers-payant	Prise en charge financière supérieure à ce qu'elle devrait être	Elevée	Utile si le contrôle biométrique non concluant conduit le professionnel de santé à refuser la délivrance du soin ou du médicament
	Utilisation de la carte Vitale d'un tiers par une personne en situation irrégulière sans être éligible à l'aide médicale d'État (AME)	Accès aux prestations de santé et, selon les droits, prise en charge financière	Elevée	Utile si le contrôle biométrique non concluant conduit le professionnel de santé à refuser la délivrance du soin ou du médicament
	Utilisation de la carte Vitale d'un tiers par une personne ayant des droits ouverts recherchant l'anonymat	Impact financier limité ; erreur dans les informations renseignées dans le dossier médical	Elevée	Utile si le contrôle biométrique non concluant conduit le professionnel de santé à refuser la délivrance du soin ou du médicament
Fraude à la condition de résidence (assurés)	Ouverture de droits au bénéfice d'une personne qui ne justifie pas d'un séjour régulier lui permettant d'être éligible à la protection universelle maladie (PUMA)	Accès aux prestations de santé et, selon les droits, prise en charge financière	Faible	La carte Vitale est utilisée par son porteur titulaire du NIR associé ; la carte Vitale est émise sur la base de droits frauduleusement ouverts. Seule la fermeture des droits permet de faire cesser la fraude
	Maintien de l'accès aux soins malgré le non-respect de la condition de résidence stable en France pour des personnes ayant déjà bénéficié de la PUMA à bon droit	Accès aux prestations de santé et, selon les droits, prise en charge financière	Faible	La carte Vitale est utilisée par son porteur titulaire du NIR associé ; la carte Vitale est émise sur la base de droits frauduleusement ouverts. Seule la fermeture des droits permet de faire cesser la fraude
Fraude à la délivrance de médicaments stupéfiants ou onéreux (assurés)		Accès à des produits de santé en vue de trafic ; bénéfice financier direct pour le fraudeur	Faible	Lorsque la carte Vitale est utilisée par son détenteur légitime, pas d'effet sur la fraude. C'est la prescription qu'il faut sécuriser
	Facturation d'actes fictifs	Prise en charge financière ; bénéfice financier direct pour le professionnels	Faible à Moyenne	En cas de complicité, pas d'effet sur la fraude. Blocage dans certains cas pour des flux sécurisés à deux cartes (Vitale et professionnelles). Capacité limitée à bloquer la facturation en cas de flux sur la base de l'empreinte de la carte
Professionnels de santé	Facturation d'actes plus coûteux que ceux effectivement réalisés (sur-cotation)	Prise en charge financière ; bénéfice financier direct pour le professionnel	Faible à Moyenne	En cas de complicité, pas d'effet sur la fraude. Blocage dans certains cas pour des flux sécurisés à deux cartes (Vitale et professionnelles). Capacité limitée à bloquer la facturation en cas de flux sur la base de l'empreinte de la carte

Source : Mission.

2. La lutte contre la fraude par l'Assurance maladie s'est renforcée à partir de 2010, conduisant à une hausse des montants détectés et recouvrés, mais des marges de progression subsistent

2.1. Approfondissant la démarche initiée en 2010, la convention d'objectifs et de gestion (COG) 2018-2022 conclue par l'État avec l'Assurance maladie a été marquée par un renforcement de la politique de lutte contre la fraude, malgré des objectifs modestes quant aux montants de fraude détectée

2.1.1. Le cadre de lutte contre la fraude défini s'est renforcé au fil des COG depuis 2010, pour atteindre un objectif de 265 M€ de fraude détectés ou évités en 2022

Depuis 1996, des **conventions d'objectifs et de gestion (COG)** sont négociées par les branches du régime général de sécurité sociale avec les administrations de l'État qui en assurent la tutelle (directions de la sécurité sociale et du budget). Ces COG leur assignent des objectifs opérationnels à atteindre et des plafonds d'effectifs et de dépenses de gestion administrative.

Depuis 2010, les COG des branches du régime général ont fixé des **objectifs de détection de préjudices au titre de fraudes**, en premier lieu à l'Assurance maladie.

Encadré 2 : Contrat d'objectif et de gestion (COG)

Les COG formalisent dans un document contractuel la délégation de gestion du service public de la sécurité sociale aux organismes gestionnaires. Elles fixent les **objectifs à atteindre et les moyens à mettre en œuvre pour moderniser et améliorer la performance du système** de protection sociale, aussi bien en termes de maîtrise des dépenses que de meilleur service rendu aux usagers. Chaque branche ou régime établit sa COG en fonction des axes stratégiques qui lui sont propres, même si les principes généraux restent les mêmes pour tous.

De portée nationale, les COG et leurs objectifs sont ensuite déclinés sous forme d'orientations opérationnelles en **contrats pluriannuels de gestion (CPG)** entre la caisse nationale et les caisses locales. Le CPG précise pour chaque domaine et pour chaque organisme, sous forme d'indicateurs, les actions concrètes à mettre en œuvre et les résultats à obtenir en tenant compte des conditions de réalisation au plan local.

Une COG couvre **une période de cinq ans**. Elle est signée par le président et le directeur de la caisse concernée ainsi que par les ministres de tutelle.

Pour la période en cours, le **COG 2018-2022 de l'Assurance maladie** est structurée autour des **cinq axes** de gestion suivants :

- renforcer l'accès au système de soins ;
- contribuer à la transformation et à l'efficacité de notre système de santé ;
- rendre aux assurés un service maintenu à un haut niveau de qualité ;
- accompagner l'innovation numérique en santé ;
- réussir l'intégration des autres régimes **en garantissant un fonctionnement efficient de la branche**.

Afin de renforcer l'efficacité de la politique de contrôle et de lutte contre la fraude, l'Assurance Maladie a notamment pris, dans le cadre de sa **convention d'objectifs et de gestion (COG) 2018-2022**, les engagements suivants :

Annexe III

- ◆ « *Élaborer une stratégie globale de contrôle* »
 - « *À cet égard, l'Assurance Maladie attachera une importance particulière à la réalisation des **contrôles associés à la mise en œuvre de la PUMa*** » ;
 - « *Afin d'optimiser les ressources consacrées aux contrôles, l'Assurance Maladie recherchera à la fois leur **plus large automatisation** [...]* » ;
- ◆ « *Renforcer l'efficacité de la lutte contre la fraude* » [...] « *l'élaboration d'un **référentiel national de LCF dans le cadre du système de management intégré (SMI)*** ».

Comme inscrit dans le COG²¹, la CNAM décline son action à travers des **plans annuels de contrôle contentieux et de répression des fraudes et des activités fautives**, complétés, à partir de 2018, de plans régionaux construits sous l'égide des DCGDR²² et des services chargés de la lutte contre la fraude au sein des CPAM.

En complément de ces engagements sur la stratégie à déployer, la COG a fixé des objectifs annuels chiffrés quant aux préjudices détectés (+3 M€, soit +1,5 % pour les préjudices subis). Ces progressions limitées sont nettement inférieures à celles des dépenses de prestations entrant dans le champ de l'ONDAM : selon la loi de financement de la sécurité sociale (LFSS) pour 2018, celle-ci devait atteindre 9,7 % en cumul entre 2018 et 2022. Depuis 2018, la lutte contre la fraude contribue aux **économies réalisées au titre de l'ONDAM**. Pour 2023, les économies attendues s'élèvent à 300 millions d'euros (soit 24,7 % des 1,213 Md € d'économies attendues sur l'ONDAM).

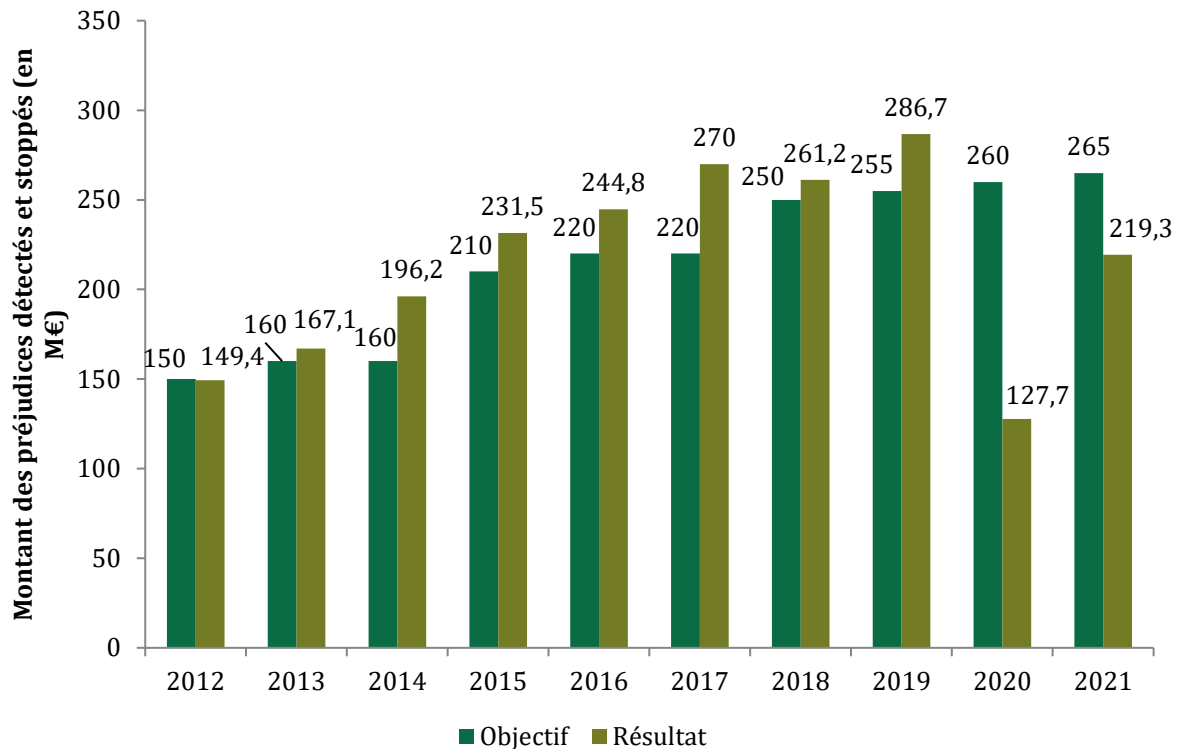
²¹ Engagement « *Élaborer une stratégie nationale de contrôle* », avec comme actions « *Élaborer un prototype de plan de contrôle sur une catégorie de professionnels de santé et une catégorie de frais de santé* » et « *Généraliser la démarche de plans de contrôle sur les principales catégories de professionnels de santé et de prestations en espèces* ».

²² Directions de la coordination de la gestion du risque.

Annexe III

Dans ces conditions, **l'objectif de préjudices subis détectés fixé pour l'Assurance maladie pour 2022 (203 M€) a été dépassé dès le premier exercice de la période de contractualisation (en 2018 et 2019)**. En 2020 et 2021, la crise sanitaire a conduit à réviser les objectifs à la baisse en cours d'exercice (cf. graphique 6).

Graphique 6 : Montant des préjudices détectés et stoppés, objectifs fixés par les COG et résultats annuels (en M€)



Source : CNAM.

2.1.2. Une prise en compte améliorée du risque de fraude, centrée sur des programmes annuels de contrôle nationaux et locaux

L'Assurance Maladie a engagé en 2017 une rénovation de sa stratégie de lutte contre la fraude (LCF) qui s'est notamment concrétisée par la mise en place des premiers plans régionaux de LCF, le renforcement de l'accompagnement de son réseau, le développement de nouveaux programmes de contrôles, l'amélioration des méthodes de détection et l'enrichissement de son dispositif de formation métier dédié à la lutte contre la fraude.

Élaboré au début de la COG 2018-2022, un **programme de rénovation de la gestion du risque « Rénov'GDR »**, a conduit à l'intégration des actions de contrôles et de lutte contre la fraude dans une acception large de la « **gestion du risque** » : prévention, maîtrise médicalisée, contrôles et lutte contre la fraude.

En particulier, **l'axe 11 de Rénov'GDR** est dédié au « *Contrôle et lutte contre les erreurs de facturation, les abus et la fraude* » désormais conduit par la DDAFF (cf. infra), tout en y associant les organismes du réseau, dans une perspective de synergie sur des sujets d'intérêt commun : évaluation des risques d'erreurs, d'abus et fraudes, évolution des dispositifs de prévention des risques et d'accompagnement des professionnels de santé, de contrôle et de lutte contre la fraude.

Annexe III

La stratégie de lutte contre la fraude s'appuie principalement sur des **programmes nationaux de contrôle contentieux qui sont structurés autour des thèmes de contrôle** suivants:

- ◆ obtention des droits ;
- ◆ prestations en espèces ;
- ◆ établissements :
- ◆ prestations en nature/frais de santé ;
- ◆ établissements / soins de ville.

Entre 2018 et 2021, **90 programmes de contrôle** ont été lancés sur ces thématiques (cf. tableau 12), majoritairement sur les prestations en nature/frais de santé ainsi que les prestations en espèces, dès lors que les programmes de contrôle des établissements de santé ont été depuis 2020 suspendus ou très partiellement réalisés.

Les programmes nationaux sont pilotés par la caisse nationale : celle-ci met à disposition des caisses locales les **kits de requêtes** (par exemple, pour le plan de contrôle de la résidence des bénéficiaires de la PUMA, cinq requêtes sont diffusées dont les requêtes multi-hébergeurs, parents de jeunes enfants de moins de six ans, assurés ayant des soins regroupés sur un mois.).

Les organismes locaux sont également associés à l'élaboration des programmes nationaux, **les résultats des programmes régionaux permettant d'alimenter la construction de programmes nationaux**, dès lors qu'un même type de fraude est détecté dans plusieurs régions et peut s'exprimer dans d'autres. Ces programmes sont ensuite déclinés au sein de chaque thématique²³.

En 2021, la CNAM a présenté une nouvelle stratégie de contrôle et de lutte contre la fraude. Un **plan national bisannuel 2021-2022 de lutte contre la fraude**, a été élaboré selon les orientations fixées dans le plan d'actions ministériel de lutte contre les fraudes sociales 2021-2022 piloté par la direction de la sécurité sociale. Il intègre également les nouvelles fraudes liées à la crise sanitaire et suit les recommandations issues des rapports parlementaires relatifs à la lutte contre la fraude publiés à l'automne 2020²⁴.

De nouveaux programmes de contrôle ont été lancés pour faire face aux risques émergents (internet, réseaux sociaux, fraudes au niveau interdépartemental, dans les DOM, en bande organisée).

Tableau 12 : Programmes annuels de contrôle contentieux lancés entre 2018 et 2021

Exercice	Obtention des droits	Prestations en espèces	Établissements de santé	Prestations en nature/Frais de santé	Établissements de santé/soins de ville	Total par an
2018	2	5	5	10	0	22
2019	2	5	6	14	2	29
2020	2	8	1	10	0	21
2021	2	6	1 (HAD)	9	0	18
Total par thème	8	24	13	43	2	90

Source : Mission, à partir des données des bilans annuels de la politique de lutte contre la fraude et les activités fautives établis par l'assurance maladie conformément à l'article L. 114-9 du code de la sécurité sociale.

²³ A titre d'exemple : contrôle contentieux sur l'activité des transporteurs sanitaires, sur la résidence des bénéficiaires de la PUMA, s'agissant des indemnités journalières : cumul indemnités journalières/activité rémunérée, employeurs atypiques, etc.

²⁴ Rapport de la commission d'enquête relative à la lutte contre les fraudes aux prestations sociales, Assemblée nationale, septembre 2020.

L'accent est mis sur l'évaluation de la fraude, le renforcement des échanges de données entre organismes, le déploiement de programmes nationaux à visée dissuasive sur les nouveaux droits ou nouvelles prestations et la mise en place de sanctions plus lourdes envers les fraudeurs. Il comprend **quatre axes** :

- ◆ évaluer la fraude ;
- ◆ rénover la politique de contrôle des trafics de médicaments ;
- ◆ poursuivre le programme national de contrôle de la filière visuelle ;
- ◆ lutter contre le détournement du modèle des centres de santé en en contrôlant l'installation et le conventionnement.

La **politique de contrôle des prestations remboursées** doit également être rénové permettant d'optimiser les processus de contrôles à tous les niveaux : détection optimisée, évaluation renforcée contrôles pédagogiques à visée préventive, contrôles *a priori*, contrôles *a posteriori* et lutte contre la fraude et abus :

- ◆ poursuite pour les infirmiers libéraux et extension aux masseurs-kinésithérapeutes de la stratégie globale d'accompagnement et de contrôle à l'attention des professionnels libéraux en primo-installation (environ 10 millions d'euros) ;
- ◆ analyse *a posteriori* de la facturation des professionnels via des outils de requêtage automatisés permettant de déclencher des actions contrôles ciblés ou de lutte contre la fraude mais également des campagnes d'accompagnement (impact évalué à 5 M€) ;
- ◆ contrôles *a priori* avec la mise en place de contrôles embarqués sur les actes facturés par les professionnels de santé (environ 20 millions d'euros) ;
- ◆ contrôles *a posteriori* sur le respect des règles de facturations des actes médicaux et paramédicaux (environ 20 millions d'euros) ;
- ◆ programme annuel de lutte contre la fraude et les pratiques fautives et abusives pour un montant d'environ 200 millions d'euros. »²⁵).

L'assurance maladie a mis en place deux types de requêtes :

- ◆ **une première requête permettant d'identifier sur la base ERASME SIAM les rejets et signalements générés par l'utilisation d'une carte vitale en opposition.** Si une FSE émise à partir d'une carte frauduleuse, abusive ou opposable est traitée par la chaîne de liquidation du CTI (IRIS), l'état de la carte est détecté par la liste d'opposition remontante (LOR), et la FSE fait l'objet d'un signalement ou d'un rejet selon le cas. L'exploitation de ces rejets et de ces signalements permet :
 - de contacter l'assuré afin de lui demander si les soins le concernent (ou l'un de ses ayants droit) ;
 - d'engager les procédures de récupération de la carte Vitale interdite selon les consignes décrites dans la circulaire CNAM²⁶ ;
 - de suivre le respect de l'utilisation du système d'opposition par les professionnels de santé, afin de leur garantir le remboursement de leurs factures en cas de dispense d'avance des frais.
- ◆ **une seconde requête permettant de détecter les éventuelles situations de rétention d'une carte Vitale par le professionnel de santé.**

²⁵ Source : Rapport « Améliorer la qualité du système de santé et maîtriser les dépenses : les propositions de l'Assurance Maladie pour 2023 »

²⁶LR-DFC-54/2006 du 26/10/2006.

Annexe III

Outre ce qui précède, il n'existe pas de contrôle spécifique sur atypie à partir du seul critère de consommations de soins par les assurés. La technique de détection par atypie sert à alimenter des observatoires afin d'élaborer des profils de professionnels de santé atypiques pour orienter les contrôles.

De même, il n'y a pas de contrôles par type de consommations atypiques (par exemple, consommation de soins élevée pour des assurés, volume d'actes médicaux ou montants d'honoraires supérieurs à la moyenne pour les professionnels de santé de même catégorie). **Les contrôles restent orientés vers les anomalies tirées de l'analyse des facturations.**

Le reporting des programmes nationaux s'effectue au fil de l'eau par l'outil de suivi OG3S (Outil de gestion des signalements et de leurs suites) : diffusé en 2012 et généralisé en 2013, cet outil repose sur une base unique qui permet :

- ◆ **le suivi mensuel des résultats** de la mise en œuvre de chaque programme auquel est affecté un « code programme » puis la consolidation nationale annuelle sur cette base des objectifs CPG (préjudice subi et évité, partiellement taux de suites contentieuses) ;
- ◆ **l'échange instantané d'informations entre les différentes caisses** sur un dossier commun.

2.1.3. La CNAM a fait évoluer son organisation dédiée à la lutte contre la fraude et a maintenu les moyens humains dédiés autour de 2% des effectifs

Lors de la signature du COG 2018-22, le pilotage des actions de contrôle et de lutte contre la fraude était assuré par deux directions :

- ◆ d'une part, la **direction de l'Audit, du Contrôle-Contentieux et de la Répression des Fraudes (DACCRF)** comprenant **cinq départements métiers** (département de l'audit général, département investigations établissements, département investigation ville et accès aux droits, département détection statistique et département du droit des contentieux) **et deux départements de coordination de lutte contre la fraude** (département efficacité et département accompagnement et professionnalisation) ;
- ◆ d'autre part, la **direction déléguée des finances et de la comptabilité (DDFC)** comptant **six départements** en gestion directe, dont un département d'audit, dit de validation des comptes et un département en charge de la définition de la politique de contrôle interne comptable, dit de prévention, maîtrise des risques et réglementation financière.

Initié à partir du lancement fin 2020 du programme de rénovation de la gestion du risque, Rénov'GDR, **le processus de rapprochement des deux directions est devenu opérationnel en 2022**. Ce rapprochement fonctionnel a pour objectif de faciliter les synergies et la transversalité des compétences, d'optimiser les activités de contrôle et de lutte contre la fraude d'une part, d'audit d'autre part.

La nouvelle **direction déléguée de l'audit, des finances et de la lutte contre la fraude (DDAFF) comprend quatre services** (et un département directement rattaché à la direction sur le droit des contentieux) :

- ◆ audit;
- ◆ système d'information ;
- ◆ comptabilité et trésorerie ;

Annexe III

- ◆ contrôle/lutte contre la fraude²⁷.

Au total, les **effectifs affectés à la lutte contre la fraude s'établissent à 1 434 ETP en 2022**, en baisse au cours des cinq dernières années (-12 %, cf. Tableau 13). Ces effectifs représentent 1,47 % des effectifs en ETP de l'Assurance maladie en 2021²⁸.

Tableau 13 : Effectifs du régime général d'assurance maladie consacrés à la lutte contre la fraude entre 2018-2022

Effectifs	2017	2018	2019	2020	2021	2022
ETP Service administratif	937	1 051,5	1 069,1	818,3	909	1 005
ETP Service médical	566	578,5	565,9	418,7	401	429
Total	1 503	1 630	1 635	1 237	1 310	1 434

Source : CNAM

Une enquête-questionnaire a été adressé par la DDAFF au réseau afin de **recenser plus précisément le nombre d'agent dédiés au processus lutte contre la fraude**, et les catégories de métiers (requêteurs, investigateurs administratifs, agent enquêteur, juriste..). Les résultats de cette enquête devraient être disponibles en avril 2023.

Le tableau ci-dessous montre que la **part des effectifs affectés au processus fraudes dans l'ensemble des processus de gestion de l'assurance maladie est restée relativement stable durant la COG** : de 2,1% en 2018, il a légèrement augmenté en 2019 avant de connaître une baisse en 2020, liée probablement à l'affectation d'une partie des effectifs sur des activités liées à la crise sanitaire, puis de remonter à nouveau pour atteindre **1,8% en 2022**.

Depuis 2017, les effectifs administratifs consacrés à la lutte contre la fraude au sein de la CNAM affichent une quasi-stabilité, passant de 937 à 909 ETP (-3%) entre 2017 et 2021, décomposée en deux périodes distinctes : un renforcement initial des effectifs entre 2017 et 2019 (+ 132 ETP, + 14%) avant une baisse pendant la période de la crise (-160 ETP, - 15% de 2019 à 2021).

Au niveau de chaque caisse, les effectifs consacrés à la fraude peuvent être limités à quelques agents, alors même que les investigations et les contrôles sur place nécessitent un temps agent important, surtout dans un contexte de complexification des types de fraude.

La volumétrie des dossiers à investiguer pour chaque caisse, qui tient compte du nombre d'assurés sur critère de résidence, est transmise chaque année à chaque DCGDR²⁹ chargée de coordonner le déploiement des programmes de contrôle.

Quant aux profils des équipes de la CNAM dédiées à la lutte contre la fraude, ils sont très variés : statisticiens, requêteurs, investigateurs administratifs, agents agréés assermentés ou juristes. Malgré tout, compte-tenu de l'évolution des types de fraude, de même que des techniques d'investigation, **certains profils font défaut, notamment des agents disposant à la fois d'une expertise en datamining** et d'une bonne connaissance du système d'information (complexe) de l'Assurance maladie.

Par ailleurs, les professionnels de santé sont soumis à des obligations déontologiques de lutte contre la fraude (cf. Tableau 14).

²⁷ Le service de contrôle et de lutte contre la fraude regroupe sept départements : prévention, maîtrise des risques et réglementation financière ; investigations ville et accès aux droits ; investigation établissements ; détection statistique ; accompagnement et professionnalisation ; efficacité.

²⁸ 1310/ 89 147 ETPMA Assurance maladie. Source : LFSS 2023- annexe 10

²⁹ Direction de la coordination de la gestion du risque

Annexe III

Tableau 14 : Obligations déontologiques des professionnels de santé dans la lutte contre la fraude

Profession	Article du Code de la santé publique	Texte applicable
Chirurgiens-dentistes	R. 4127-221	Sont interdits : 1° Tout acte de nature à procurer à un patient un avantage matériel injustifié ou illicite ; 2° Toute ristourne en argent ou en nature faite à un patient ; 3° Tout versement, acceptation ou partage de sommes d'argent entre des praticiens ou entre des praticiens et d'autres personnes sous réserve des dispositions propres aux sociétés d'exercice en commun de la profession ; 4° Toute commission à quelque personne que ce soit.
Infirmiers	R. 4312-81	Sont interdits toute fraude, tout abus de cotation ou indication inexacte portant sur les actes effectués.
Masseurs-kinésithérapeutes	R. 4321-77	Le masseur-kinésithérapeute s'abstient, même en dehors de l'exercice de sa profession, de tout acte de nature à déconsidérer celle-ci
Médecins	R. 4127-29	Toute fraude, abus de cotation, indication inexacte des honoraires perçus et des actes effectués sont interdits.
Pédicures podologues	R. 4322-43	Sont interdits au pédicure-podologue : <ul style="list-style-type: none"> ▪ tout acte de nature à procurer à un patient un avantage matériel injustifié ou illicite ; ▪ toute sollicitation ou acceptation d'un avantage en nature ou en espèces sous quelque forme que ce soit, d'une façon directe ou indirecte, pour un acte quelconque, hors les cas prévus par les articles L. 1453-6 et L. 1453-7 ; ▪ toute fraude, abus de cotation, indication inexacte des honoraires perçus ou des actes effectués.
Pharmaciens	R. 4235-9	Dans l'intérêt du public, le pharmacien doit veiller à ne pas compromettre le bon fonctionnement des institutions et régimes de protection sociale. Il se conforme, dans l'exercice de son activité professionnelle, aux règles qui régissent ces institutions et régimes.
Sages-femmes	R. 4127-337	Toute fraude, abus de cotation, indication inexacte des honoraires perçus et des actes effectués sont interdits.

Source : Code de la santé publique.

2.2. Le renforcement de la détection de la fraude s'est appuyé sur l'élaboration de cartographie des risques

L'Assurance Maladie s'est par ailleurs engagée depuis 2018 dans un travail de **cartographie des risques** qui contribue à une plus grande connaissance et donc une meilleure maîtrise des risques. Ce travail d'étude approfondi constitue une première étape nécessaire à l'évaluation chiffrée de la fraude tant elle permet de mieux connaître, pour chaque acteur ou chaque prestation analysée, les risques en termes de pratiques frauduleuses ou fautives.

Chaque cartographie recense en effet **l'ensemble des risques liés à un acteur ou à une prestation en précisant le niveau de vulnérabilité de l'Assurance Maladie et les hiérarchise en fonction de leur prévalence et de leur impact**, tant sur le plan financier que juridique.

Annexe III

L'analyse du risque passe par l'élaboration d'un état des lieux de la cible étudiée puis la description en détails de chaque processus. Les cartographies révèlent que les risques peuvent être :

- ◆ **externes**, par exemple liés aux conditions d'exercice, aux erreurs de prescriptions et de cotations des actes ;
- ◆ **internes**, par exemple liés à la gestion des flux, ou enfin associés à la réglementation comme les dispositifs conventionnels ou la codification.

Inscrite dans la stratégie de contrôle et de lutte contre la fraude, la cartographie contribue à concevoir et à planifier des programmes nationaux, tant en amont par des actions de maîtrise médicalisée, qu'en aval dans la lutte contre la fraude et les activités fautives ou abusives. La cartographie relative à la C2S (ex-CMU-C) élaborée en 2018 a notamment permis de repenser la communication externe auprès des assurés, de mieux les accompagner dans leurs obligations déclaratives et donc de limiter les risques d'erreur.

Les cartographies relatives aux EHPAD, SSIAD, rentes ATMP ont aussi été actualisées durant la période de la COG.

Huit cartographies ont déjà été mises à disposition des organismes du réseau d'Assurance Maladie :

- ◆ les infirmiers ;
- ◆ les transporteurs ;
- ◆ les bénéficiaires de la C2S, la complémentaire santé solidaire (ex-CMU-C) ;
- ◆ la tarification à l'activité (T2A) ;
- ◆ les indemnités journalières ;
- ◆ les masseurs-kinésithérapeutes ;
- ◆ les rentes invalidité / allocations supplémentaires d'invalidité (ASI)
- ◆ la prestation universelle maladie (PUMa) ;

D'autres cartographies sont en cours d'élaboration :

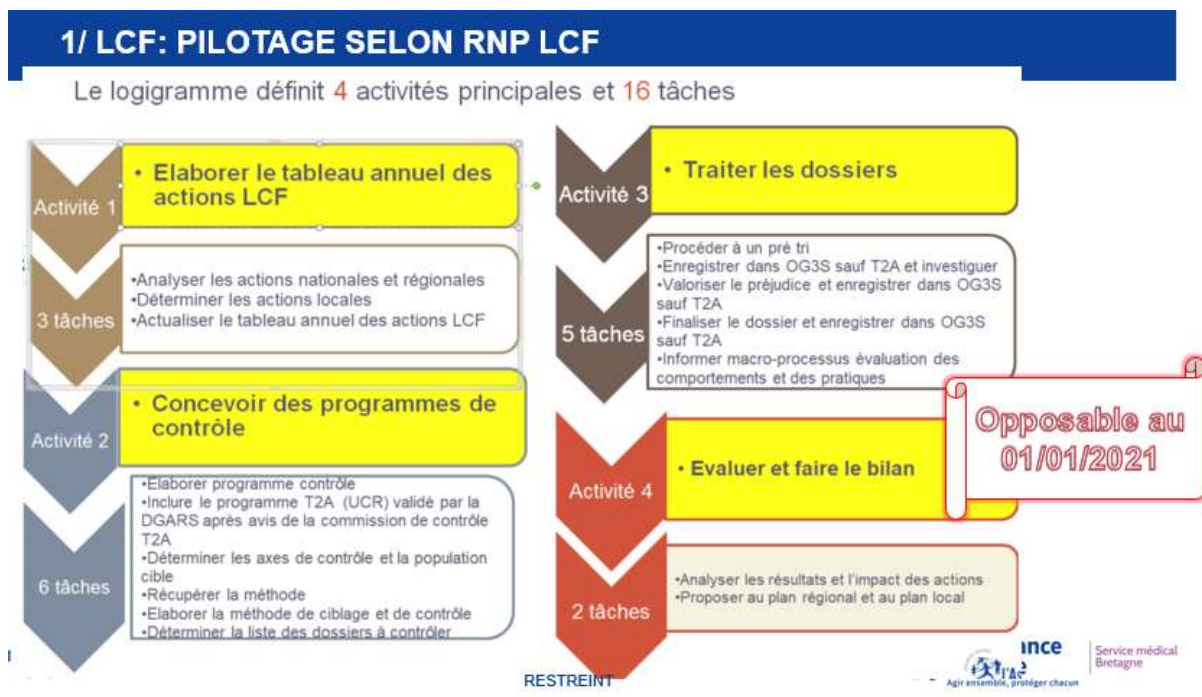
- ◆ les prestataires de soins et dispositifs médicaux (PSDM) ;
- ◆ les établissements d'hébergement pour personnes âgées dépendantes (EHPAD) ;
- ◆ les rentes accidents du travail / maladies professionnelles.

La CNAM a élaboré un **référentiel national de processus (RNP)**³⁰, expérimenté en 2019 et rendu opposable en 2021, soit un an après la date initialement prévue compte-tenu de la crise sanitaire. Après une première version intégrant les phases de détection et d'investigation, les décisions ainsi que les suivis de nature contentieuse ont été intégrés en 2020 avant la diffusion du référentiel l'année suivante.

Le référentiel se décline en quatre activités principales à mettre en œuvre de manière séquentielle (cf. Graphique 7). Ces activités sont associées à seize tâches, par exemple déterminer les actions locales, déterminer les axes de contrôle et la population cible, analyser les résultats et l'impact des actions. **Cette démarche va dans le sens d'un renforcement des capacités d'analyse, d'une harmonisation des pratiques et donc d'une réduction des écarts de performance entre les organismes du réseau.**

³⁰ Les référentiels nationaux de processus sont des outils de pilotage de processus qui constituent l'ossature du système de management intégré (SMI). Ces RNP viennent compléter les anciens plans de maîtrise socle (PMS) – reposant principalement sur le contrôle de qualité des processus – par l'intégration de nouveaux indicateurs mesurant l'efficacité, l'efficience et indicateurs de couverture des compétences. Ces nouveaux référentiels assurent une avancée dans le processus de détection et de maîtrise des risques dans la mesure où ils ont un champ élargi et coordonné (le RNP est unique pour l'ensemble des organismes), les méthodes d'analyse des risques sont renforcées, ils offrent une plus grande visibilité.

Graphique 7 : Référentiel national de processus (RNP) de lutte contre la fraude (LCF)



Source : CNAM.

2.3. Des mesures ont été prises depuis 2004 pour réduire les risques de délivrance frauduleuse de cartes Vitale

Plusieurs mesures ont été prises depuis 2004 pour réduire les risques liés à la délivrance de la carte et sécuriser le système d'émission des cartes et les facturations³¹ :

- ♦ création d'une liste d'opposition des cartes Vitale ;
- ♦ émission d'une nouvelle génération de cartes Vitale avec photo (Vitale 2) ;
- ♦ mise en place d'un portail inter-régimes qui permet d'éviter l'émission d'une nouvelle carte si l'ancienne n'a pas été restituée ou invalidée ;
- ♦ mise en fin de vie des cartes Vitale dont les titulaires n'ont plus de droits ou dont les titulaires sont décédés ou radiés.

2.4. Un renforcement récent des systèmes d'information, conçus en interne à l'Assurance maladie, a été opéré afin de faciliter la détection et l'investigation des fraudes

Pour cette sous-partie, la mission s'est appuyée sur les travaux détaillés du rapport de novembre 2022 n° 2022-027R d'évaluation de la COG CNAM 2018-2022 de l'IGAS.

L'Assurance maladie a déployé divers systèmes d'information facilitant la détection et l'investigation des fraudes. Certains sont dédiés à une profession de santé particulière tandis que d'autres ont une vocation transversale. Employés par les équipes dédiées à la lutte contre la fraude dans les CPAM, ils permettent d'orienter et de mieux cibler les travaux de contrôle.

- ♦ les outils de détection : Profileur, PSOI, GepHI :

³¹ Cf. Annexes I et II.

Annexe III

- conçu par la région Picardie en 2011 puis déployé nationalement en 2014, **PROFILEUR permet de cibler des professionnels de santé présentant des pratiques atypiques suspectes de fraude à partir des données du RIAP** (Relevé Individuel d'Activité et de Prescriptions) et à l'aide de modules permettant des sélections multicritères, des cartographies, des classements. L'outil intègre actuellement 24 professions ou spécialités³². L'outil permet également de traiter les signalements et d'être un appui aux investigations à partir de la consultation de la fiche profil du professionnel. Cet outil a évolué en 2019 pour permettre aux utilisateurs d'affiner les ciblage de profils atypiques et leur fournir de nouveaux formats de restitution. Il est dorénavant utilisé par l'ensemble des services fraudes du réseau.
 - en outre, le **système PSOI (Profil Statistique et Observatoire Individuel de la profession infirmiers) élaboré par la CPAM des Pyrénées-Orientales** dans le cadre de la Mission Déléguée 24 (MD24) a été récemment déployé nationalement pour être notamment utilisé par le réseau dans le cadre des **contrôles ciblés sur les infirmiers en 2022** et de la nouvelle stratégie de contrôles gradués des professionnels de santé. Il permet, comme l'outil PROFILEUR, de réaliser des ciblage de professionnels en fonction de risques prédéfinis et de parcours de soins d'assurés.
 - enfin, en 2022, la **CNAM a diffusé un outil open source d'analyse et de visualisation sous forme de graphiques (GepHI)**. S'appuyant sur des algorithmes de détection de communautés, sur la thématique du médicament, il permet de mettre en exergue des groupes de médecins prescripteurs/pharmaciens fortement liés entre eux par leur patientèle commune et ainsi mettre en lumière de potentiels trafics en réseau.
- ◆ les outils d'investigation : Oceanic, Cactus, Karle :
- **l'outil de contrôle et d'analyse des infirmiers ciblés Oceanic** présente le profil du professionnel, son agenda, la liste de ses patients, la visualisation des prescriptions disponibles avec une comparaison des actes facturés, il **alimente directement un tableau d'anomalies**.
 - pour les investigations concernant les transporteurs sanitaires, **l'outil de contrôle automatisé des caisses sur les transporteurs sanitaires (Cactus)**, permet le contrôle des kilomètres facturés et des horaires de transports à partir d'un distancier de référence et d'un distancier dérogatoire.
 - en outre, pour les contrôles de la profession de masseur-kinésithérapeute, **l'outil KARLE d'aide au contrôle d'activité des masseurs-kinésithérapeutes** présente un profil automatisé par requêtes et permet de visualiser des prescriptions et de les comparer aux actes facturés.
 - en remplacement de ces trois outils (Oceanic, Cactus et Karle), la CNAM prévoit **Adagio, un nouvel outil unique diffusé au réseau en fin de l'année 2022**.

Le déploiement de ces outils décline l'engagement de la CNAM inscrit dans la COG 2018-2022 visant à **renforcer l'efficacité de la lutte contre la fraude par l'élargissement du périmètre des investigations** en utilisant des nouveaux outils ou méthodes. Ces outils, même s'ils ne visent qu'un certain type d'activités et donc de fraude, offrent aux organismes locaux des moyens d'investigation et de détection plus nombreux.

³² Notamment infirmiers, masseurs-kinésithérapeute, chirurgiens-dentistes, médecins généralistes, ophtalmologues, radiologues, cardiologues.

Les temps d'analyse et d'investigation de la part des équipes à partir de ces outils sont importants, surtout au regard du nombre de programmes de contrôle concernant les professionnels de santé déployés chaque année. Ils nécessitent aussi des compétences spécifiques pour rendre leur manipulation plus efficace.

2.4.1. Le croisement des bases de données de la CNAM avec celles d'autres administrations est un outil puissant, notamment pour lutter contre la fraude à l'identité et à la résidence

Le rapport IGAS-IGF relatif aux enjeux d'intérêt commun aux branches du régime général de 2021³³ a constaté les efforts déployés ces dernières années dans la construction et l'usage de systèmes d'information transverses et partagés :

- ◆ système national de gestion des identifiants (SNGI) ;
- ◆ déclaration sociale nominative (DSN) ;
- ◆ dispositif de ressources mutualisées (DRM) ;
- ◆ répertoire de gestion des carrières unique (RGCU) ;
- ◆ **répertoire national commun de la protection sociale (RNCPS)** ³⁴ ;
- ◆ PNDS.

La mission considérait toutefois, « *dans le sillage de plusieurs rapports récents des inspections générales, qu'il subsiste une sous-potentialisation dans l'usage ou le périmètre de ces outils* », qui au-delà de l'enjeu de rationalisation de la gestion des développements de SI et de facilitation de la relation aux usagers, ont un **intérêt important pour éviter la fraude** (permettant la récupération directe de données des assurés) **ou la détecter** (pour vérifier, par exemple avec le RNCPS³⁵, la véracité des informations transmises par l'utilisateur avant l'ouverture d'un droit).

Le **plan d'actions interministériel de lutte contre les fraudes sociales 2021-2022 prévoit de renforcer la démarche d'échanges de données entre organismes sociaux et avec d'autres partenaires** (services fiscaux, ministère de l'intérieur...) encore considérés comme insuffisants. Cette démarche porte en particulier sur les processus suivants :

- ◆ immatriculation et identification ;
- ◆ contrôle de l'existence et certifications des droits ;
- ◆ contrôle de la condition de résidence ;
- ◆ contrôle des conditions de ressources.

Par ailleurs, un **protocole visant à améliorer les échanges d'informations entre le ministère de l'intérieur et les organismes de protection sociale, en matière de lutte contre la fraude documentaire et à l'identité** a été signé le 1^{er} décembre 2021. Il propose aux organismes de protection sociale une offre d'outils techniques et numériques de détection.

³³ Rapport IGAS N°2021-042R et IGF N°2021-M-022-02 « Les enjeux d'intérêt commun aux branches du régime général de la sécurité sociale »

³⁴ Base de données utilisée pour la vérification des conditions d'attribution d'une aide créée par l'article 138 de la loi 2006-1640 du 21 décembre 2006 créant l'article L. 114-12-1 du Code de la sécurité sociale, centralisant les données sur les allocataires des différents organismes de protection sociale français, sur la base du NIR.

³⁵ Cf. rapport IGAS n°2021-011 d'évaluation du répertoire national de protection sociale (RNCPS) : bilan et perspectives, établi par B. Ferras et C. Lépine

Annexe III

Toutefois, les organismes sociaux n'ont pas accès ou n'exploitent pas certaines données détenues par des administrations de l'État pour contrôler la stabilité de la résidence en France (registre des Français établis à l'étranger, bases élèves) ou le caractère irrégulier du séjour (visas de court séjour pour le contrôle de l'aide médicale de l'État, dont l'attribution est conditionnée par ce caractère irrégulier).

L'assurance maladie a aussi accès, pour ses travaux de vérification (par exemple en préalable à l'ouverture de droits à la C2S) et d'investigation en cas de soupçon de fraude, à certaines données mises à disposition par d'autres administrations, telles que la **direction générale des finances publiques** (DGFIP)³⁶, qui donne aux organismes de sécurité sociale accès notamment à :

- ◆ FICOBA (qui permet l'accès aux comptes bancaires ouverts en France par les personnes physiques ou morales, dont les comptes-épargne et les compte de titres) ;
- ◆ FICOVIE (qui donne accès aux contrats de capitalisation ou de placement, notamment les contrats d'assurance vie d'un montant supérieur ou égal à 7 500€).

Elle a aussi accès aux données mises à disposition par le **ministère de l'Intérieur** telles que :

- ◆ DOCKERIF (titres d'identité) ;
- ◆ VISABIO (données sur les vis s délivrés) ;
- ◆ AGDREF (dossiers des ressortissantes étrangers en France).

Les outils internes s'avèrent toutefois présenter certaines limites. En premier lieu, les bases de données nationales et locales étant différentes, la caisse nationale rencontre des **difficultés à concevoir des requêtes clés en main pour les organismes du réseau**.

Par ailleurs, **l'antériorité des données utilisées dans le système informationnel ERASME est limitée à 2 ans et le trimestre en cours, ce qui est plus court que la prescription en matière de fraude (cinq ans)**. Lors d'échange avec la mission, la CNAM a indiqué que le doublement de la durée de conservation aurait un coût élevé du fait de la nécessité de disposer de bases de stockages élargies. Par ailleurs, il a été précisé que lors du lancement d'investigations complexes et de grande ampleur (dont l'instruction peut durer un ou deux ans), une copie des données contenues dans ERASME était effectuée, afin de disposer de données plus anciennes) lors de la conclusion de l'enquête (deux ans et un trimestre auxquels s'ajoutent les données recueillies pendant la période d'instruction).

Concernant **l'outil OG3S, l'accès par les échelons national et régionaux au détail des dossiers traités par les organismes locaux est à l'heure actuelle restreinte** à celles nécessaires aux analyses statistiques (anonymisation des dossiers, pas d'antériorité des dossiers contrôlés pour lesquels aucune fraude ou faute n'a été détectée...). Le pilotage plus fin et la coordination d'un certain nombre de contentieux et d'actions de contrôle se trouvent obérés par cette limitation.

2.4.2. La mobilisation des task force nationales en cas de fraudes à forts enjeux

Une dizaine de task forces nationales (TFN) ont été déployées depuis 2018 sur différentes thématiques³⁷. Ces équipes ont par ailleurs été fortement mobilisées pendant la période de crise sanitaire du fait des fraudes aux attestations de vaccination, aux tests de dépistage. En outre, les TFN réalisent environ 4 à 5 soutiens techniques d'équipes locales par an.

³⁶ L'accès aux données de la DGFIP à des fins de lutte contre la fraude est encadré par l'article 6 de la loi n° 2018-898 du 23 octobre 2018 relative à la lutte contre la fraude.

³⁷ Patients pris en charge en oncologie, la dialyse rénale, les soins à domicile de patients en fin de vie, les soins infirmiers et les centres de santé (ophtalmologiques et dentaires).

Annexe III

Ces task forces, dont les équipes comprennent **à la fois des agents de la caisse nationale et des organismes locaux**, sont mobilisées dans plusieurs cas de figure :

- ◆ détection de nouveaux modes opératoires de fraudes,
- ◆ dans les cas de fraudes en réseau ou bande organisée ;
- ◆ lorsqu'une fraude se diffuse sur plusieurs régions et/ou rapidement ;
- ◆ lorsqu'elle présente des enjeux financiers majeurs ou qu'il existe un besoin d'harmoniser voire de centraliser les actions contentieuses ;
- ◆ en appui à une ou plusieurs régions pour faire aboutir des plaintes pénales.

Cette organisation présente plusieurs avantages : l'équipe peut intervenir en amont dès le repérage d'une suspicion de fraude majeure ou complexe, ce qui permet de gagner en anticipation et en réactivité. Elle se traduit également par une collaboration plus étroite avec les services de police, de gendarmerie (notamment avec **l'Office Central de Lutte Contre le Travail Illégal, OCLTI**) et de justice permettant plus d'efficacité, dans la mesure où les plaintes des CPAM (toutes régions confondues) sont alors centralisées auprès d'un même parquet.

Enfin, la mise en place de task forces assure une coordination, une synchronisation et une accélération des actions de l'ensemble des CPAM à tous les stades d'avancement de la campagne de contrôle, qu'il s'agisse de mener les investigations de concert, selon les mêmes procédés et au même moment, ou qu'il s'agisse du choix et de la mise en œuvre des suites contentieuses. Ce mode d'organisation renforce les capacités d'action de l'assurance maladie dans le traitement de ces fraudes à enjeux.

2.4.3. L'utilisation des données par « datamining » et l'emploi récent de modélisations « machine learning » et d'algorithmes de reconnaissance vont permettre d'améliorer la détection des profils de fraudeurs

Le datamining et, plus récemment, le recours au big data, optimisent l'exploitation des bases de données et permettent de mieux identifier la fraude à l'obtention des droits.

Depuis 2006 la plupart des programmes de contrôles pilotés par les services de gestion du risque du réseau s'appuie sur la **détection par des méthodes statistiques de « datamining raisonné**». À partir d'une « fouille » ordonnée sur les bases de données de l'Assurance Maladie sont créés des indicateurs de ciblage en fonction de l'expérience humaine acquise sur les différents thèmes et acteurs de soins étudiés. Cette méthode consiste notamment à repérer des professionnels de santé ou assurés pour lesquels les valeurs de l'indicateur sont supérieures à un seuil défini prenant en compte une moyenne de dépenses, et un écart type afin de sélectionner les pratiques les plus aberrantes statistiquement (repérage des comportements atypiques) et ainsi retenir un nombre de contrôles compatibles avec les moyens d'investigation.

Dans cette logique d'amélioration du ciblage, **l'Assurance Maladie investit depuis 2019 dans une nouvelle approche de datamining dit « en apprentissage supervisé »** qui permet de créer des modèles mesurant *a priori* (avant investigation) la probabilité de fraude d'un acteur à partir de cas de fraudes identifiés et de cas de non fraudes. Ces méthodes permettent de modéliser différents profils de fraude et notamment de cibler des fraudeurs non repérés avec les méthodes classiques de ciblage (datamining raisonné). Le datamining « *en apprentissage supervisé* » est ainsi **utilisé depuis 2018 pour le programme national de contrôle-contentieux relatif aux bénéficiaires de la C2S sans participation financière (ex-CMUC)**.

Annexe III

Cela a permis un meilleur ciblage des dossiers à contrôler, compte-tenu de la lourdeur des contrôles à réaliser pour chaque dossier (droits de communication bancaire, procédure contradictoire) et d'accroître le montant de préjudice par dossier et d'augmenter le taux de dossiers détectés avec des éléments fautifs ou frauduleux, comparativement à celui observé avec un ciblage basé sur une approche aléatoire ainsi qu'en atteste le montant du préjudice moyen par dossier en hausse entre 2017 et 2022 (cf. Tableau 15) :

- ◆ **en 2017**, 41 337 dossiers ont été contrôlés pour un taux de fraudes et fautes de 7,02% ;
- ◆ **en 2019** avec le recours au datamining, 19 128 dossiers ont été contrôlés pour un taux de fraudes et fautes détecté de 10,24%.

Tableau 15 : Montant de préjudice moyen par dossier détecté par la CNAM entre 2017 et 2022 (en €)

2017	2018	2019	2020	2021	2022
902	949	1 048	1 093	1 243	1 305

Source : CNAM.

Des objectifs de nombre de dossiers à contrôler sont fixés chaque année aux organismes et il est demandé de contrôler a minima 50% des dossiers avec le datamining, 30% à partir de requêtes développées en local (ou de datamining) et 20% en tirage aléatoire. La conservation d'une part de contrôles en tirage aléatoire permet de faire évoluer le datamining en rajoutant des variables supplémentaires détectées à partir des dossiers contrôlés aléatoirement. Le recours au datamining a ainsi permis une meilleure détection des situations atypiques.

En 2021, de nouvelles modélisations « machine learning » de détection de fraude ont été explorées par la CNAM sur la thématique des dispositifs médicaux. Le machine learning ou apprentissage automatique est la principale technique de l'intelligence artificielle qui consiste à construire des algorithmes à partir de base d'apprentissage et de test pour leur permettre de faire des prédictions.

L'utilisation de ces différents types de modélisations pour l'analyse des dépenses de santé des bénéficiaires offre une nouvelle approche et devrait permettre, selon la CNAM, d'aboutir à un ciblage plus efficient en complément des méthodes actuelles de détection de fraude. Les résultats de ces travaux n'étaient encore connus à date.

3. Pistes d'amélioration de la lutte contre la fraude à l'assurance maladie, pour les types de fraude impliquant l'usage de la carte Vitale

Dans son rapport de septembre 2020 consacré à la lutte contre la fraude sociale, la Cour des comptes a émis plusieurs recommandations concernant la stratégie de lutte contre la fraude élaborée et mise en œuvre par l'Assurance maladie.

Parmi celles-ci figuraient des recommandations relatives aux « fraudes et autres irrégularités liées aux actes et prestations facturés à l'assurance maladie ». La Cour des comptes proposait de :

- ◆ rendre obligatoire la dématérialisation de l'ensemble des prescriptions médicales (e-prescription), y compris en établissement de santé ;
- ◆ individualiser chaque acte et prestation dans les nomenclatures tarifaires ;
- ◆ mettre en place des contrôles automatisés de l'application des règles de compatibilité et de cumul des actes et prestations facturés, ainsi que de conformité aux décisions du service médical ;
- ◆ prévoir une obligation d'intégration de ces contrôles aux logiciels de facturation des professionnels et établissements de santé ;

Annexe III

- ◆ maintenir une facturation individualisée par professionnel de ville, même salarié ;
- ◆ permettre aux caisses d'assurance maladie de consulter les données d'horodatage dans les logiciels de facturation des professionnels de santé.

La mission a pu constater l'avancement des travaux concernant certaines des mesures préconisées et considère que ces recommandations sont pertinentes pour contribuer à une meilleure détection et à une prévention renforcée de la fraude à l'assurance maladie.

3.1. Renforcer les initiatives déjà lancées par la CNAM dans le COG 2018-2022

3.1.1. Mieux sécuriser l'affiliation des assurés sociaux en amont des prestations

Depuis l'instauration de la protection universelle maladie (PUMa) au 1^{er} janvier 2016, le droit à une prise en charge des frais de santé par l'assurance maladie repose sur un **critère d'activité professionnelle ou, à défaut, de résidence régulière et stable en France**. Les personnes sans activité professionnelle, ni revenus de remplacement (retraites, pensions d'invalidité, allocations chômage), n'ont plus à solliciter le renouvellement de leurs droits.

En vue de maîtriser les risques liés à ce dispositif, un **référentiel de contrôle**, couvrant l'ensemble des régimes d'assurance maladie, a été approuvé par les ministres chargés de la sécurité sociale et du budget.

La plupart des affiliations sont vérifiées au moyen de **traitements informatisés des déclarations sociales des employeurs et des croisements automatisés d'informations** avec :

- ◆ la caisse nationale d'assurance vieillesse (CNAV) pour les pensionnés d'une retraite du régime général ;
- ◆ Pôle emploi au titre des chômeurs indemnisés ;
- ◆ la caisse nationale des allocations familiales (CNAF) au titre des titulaires de l'allocation adulte handicapé (AAH) et de la prestation partagée d'éducation de l'enfant.

En outre, la CNAM adresse à la **DGFIP** un fichier annuel afin de tenter d'appréhender la situation des **assurés pour lesquels elle ne dispose pas d'éléments justificatifs sur l'activité ou sur la résidence depuis au moins trois années**. En retour, la DGFIP lui communique :

- ◆ les personnes connues (c'est-à-dire celles ayant déclaré des revenus) ;
- ◆ les personnes connues mais n'ayant pu être rattachées à un foyer fiscal ou non identifiées avec certitude (du fait de données d'appariement pour partie non conformes) ;
- ◆ les personnes inconnues.

Les **croisements de fichiers de l'assurance maladie et de la DGFIP ainsi que, depuis 2019, du ministère de l'Intérieur (fichier AGEDREF)**, conduisent l'Assurance maladie, après demande de justificatifs aux assurés, à effectuer des **radiations de droits**.

Néanmoins, les demandes de justificatifs concernent un nombre réduit d'assurés au regard de ceux pour lesquels les conditions du maintien des droits à une prise en charge des frais de santé par l'assurance maladie sont, pour une part indéterminée d'entre eux, susceptibles de ne pas être respectées.

Annexe III

Ainsi, le plan annuel de contrôle 2019 visait **uniquement les 164 400 assurés ayant consommé des soins** au cours de l'année 2018 et des huit premiers mois de l'année 2019 **au sein des 1,14 million d'assurés sans trace d'activité ou de résidence** depuis au moins trois années, connus par la DGFIP mais non rattachés à un foyer fiscal, non identifiés avec certitude ou inconnus de cette direction. 0,9 million de bénéficiaires de la complémentaire santé solidaire étaient placés dans la même situation. Comme ceux qui l'ont précédé, **ce plan de contrôle ne couvrait ainsi pas les assurés sans données fiscales avérées n'ayant pas consommé de soins.**

En 2019, le plan annuel de contrôle contentieux et de lutte contre les fraudes a, **pour la première fois, prévu des contrôles visant à vérifier la condition de résidence de la PUMa.** Le programme national de contrôle PUMa repose sur une sélection de dossiers issus d'une requête « multi-hébergeurs », ainsi que sur des remontées de données des consulats, sur l'exploitation des signalements d'absence de résidence ou de résidence à l'étranger émanant du Centre National des Soins à l'Étranger (CNSE) ainsi que sur les échanges avec les partenaires institutionnels (CAF, Pôle Emploi, DGFIP...). Ces contrôles ont toutefois eu un **impact limité : en 2021, les fraudes à la PUMa liées à aux conditions de ressources et de résidence ont représenté 1431 dossiers traités pour un montant de préjudice subi ou évité de 9,2 M€.**

En 2021, de nouvelles requêtes de détection ont été expérimentées auprès de trois régions permettant de mieux cibler les dossiers à contrôler. Ces nouvelles requêtes ont été généralisées à l'ensemble des organismes du réseau au début de l'année 2022.

Il conviendrait donc, par divers procédés, éventuellement automatisés, d'élargir le champ des contrôles d'affiliation, et de les resserrer dans le temps, pour s'assurer que les assurés satisfont bien la condition de résidence de la PUMa.

3.1.2. Des contrôles automatisés a priori devraient être opérationnels à compter de 2023 dans le cadre du projet METEORe

La CNAM a lancé les **travaux dits « METEORe » autour de la refonte du système de tarification et de contrôle, en partenariat avec la MSA** à travers le système d'information @Tom. Plusieurs processus sont concernés :

- ◆ tarification des factures ;
- ◆ contrôle des doublons ;
- ◆ suivi de l'analyse des factures (regroupement et priorisation des diagnostics) ;
- ◆ surveillance de la facturation.

Ces travaux, qui doivent aboutir à l'issue de deux phases (en 2023 et 2024) pour la filière pharmacie ont pour objectif de renforcer de manière pérenne et continue, les dispositifs de contrôle visant à **améliorer la maîtrise du processus de traitement des frais de santé et concourir au juste paiement des factures** pour les deux organismes. Ils concourent notamment à l'amélioration de la gestion du risque et de la qualité de service vis-à-vis des assurés et des offreurs de soins. **Cela se traduit au niveau informatique par :**

- ◆ une première phase pour la **filière pharmacie en 2023** :
 - l'installation et l'**enrichissement du moteur de tarification et d'analyse de factures** dans le système d'information de l'Assurance Maladie afin d'augmenter la capacité d'automatisation, notamment la gestion automatique de la garantie de paiement et de la continuité de paiement, et d'élargir l'étendue des contrôles.
 - Les **contrôles embarqués** sont au nombre d'environ 1 400 (potentiel extensible) et portent notamment sur :
 - les **droits** : régime, **carte Vitale**, ATMP ;
 - les **actes** : bénéficiaires, OS, **taux de remboursement** ;

Annexe III

- la **facturation** : contexte, destinataire paiement, période-date ;
- le **panier de soin** : **prise en charge**, prévention ;
- le **montant** : prix unitaire, parcours de soins, **exonération** ;
- les **référentiels** : codage affiné, OS, prestations.

Ils devraient notamment permettre d'améliorer et d'automatiser le ciblage dossiers à contrôler en fonction de paramétrage définis dans l'outil de facturation en évitant de faire reposer la conduite de cette sélection sur les effectifs dédiés à l'analyse et au suivi des dossiers.

- ◆ une seconde phase dont l'ouverture de service, également sur la **filière pharmacie, est prévue en 2024** :
 - l'installation d'une nouvelle solution de contrôle inter-facture avec une **augmentation progressive de la profondeur d'historique du moteur de contrôle de doubles** pour atteindre 27 mois à terme (90 jours actuellement) ;
 - l'installation d'une **nouvelle solution de surveillance des factures** devrait permettre la surveillance automatique des activités et/ou comportement atypiques sur la base du paramétrage de critères nationaux et/ou locaux. Cette solution permettra également la gestion au niveau national des paramètres de surveillance et le renforcement de la capacité d'action des contrôleurs *a priori*.

3.1.3. Poursuivre l'effort de professionnalisation des équipes dédiées à la lutte contre la fraude et renforcer la diversité des profils recrutés pour s'adapter aux nouveaux enjeux de la fraude

Les task forces nationales (TFN) déployées par la CNAM depuis 2018 sont une étape importante dans la prise en compte des fraudes complexes et à enjeux (cf. 2.4.2).

Ces task forces, dont les équipes comprennent **à la fois des agents de la caisse nationale et des organismes locaux**, sont mobilisées dans plusieurs cas de figure :

- ◆ détection de nouveaux modes opératoires de fraudes,
- ◆ dans les cas de fraudes en réseau ou bande organisée ;
- ◆ lorsqu'une fraude se diffuse sur plusieurs régions et/ou rapidement ;
- ◆ lorsqu'elle présente des enjeux financiers majeurs ou qu'il existe un besoin d'harmoniser voire de centraliser les actions contentieuses ;
- ◆ en appui à une ou plusieurs régions pour faire aboutir des plaintes pénales.

Ce mode d'organisation renforce les capacités d'action de l'assurance maladie dans le traitement de ces fraudes à enjeux, à l'instar du service national de lutte contre la fraude à enjeux mis en place par la Caisse nationale d'allocations familiales (cf. encadré 4).

Encadré 3 : Lutte contre la fraude au sein de la Caisse nationale d'allocations familiales (CNAF)

La CNAF compte 35 200 salariés. En 2021, 95,5 milliards d'euros de prestations ont été versées et ont donné lieu à 35,6 millions de contrôles concernant 7,1 millions d'allocataires contrôlés au moins une fois, avec 100 044 lettres de mise en garde envoyées par les CAF. En 2021, la fraude détectée concernait 43 208 dossiers pour un montant de 309 millions d'euros (255,5 millions d'euros en 2020). et un préjudice moyen de 7 162 euros (6 921 euros en 2020).

700 contrôleurs sont rattachés aux CAF. Il s'agit d'agents assermentés devant le Tribunal d'instance et titulaires d'une carte professionnelle

Depuis 2010, la branche famille effectue une enquête **annuelle d'évaluation du paiement à bon droit et de la fraude (PBDF)**, portant sur la quasi-totalité des prestations légales versées, qui vise à estimer les montants d'indus frauduleux versés au titre d'une année, qu'ils aient ou non été détectés par les contrôles mis en œuvre sur les données déclarées par les allocataires.

Depuis 2021, afin de renforcer sa politique de lutte contre la fraude, la CNAF a organisé un **service national de lutte contre la fraude à enjeux (SNLFE), constitué de 30 contrôleurs répartis sur cinq CAF³⁸**, à partir de **recrutements internes** pour moitié (contrôleurs chevronnés, gestionnaires conseil allocataire, gestionnaires maîtrise des risques), mais aussi de **recrutements externes** ayant des profils variés (policiers, gendarmes, militaires, membres de l'administration fiscale, agents des URSSAF).

Le recrutement externe de profils spécialisés issus d'univers professionnels tels que la police ou la justice, ou bien d'univers professionnels sensibles à la problématique de la fraude (banque, services fiscaux) peut faciliter le travail d'investigation et la collaboration entre partenaires institutionnels.

Ces contrôleurs bénéficient d'une formation spécifique ainsi que de connaissances techniques et d'outils dédiés. Ils sont agréés par le directeur général de la CNAF à l'issue d'une formation qualifiante nationale qui s'effectue en alternance. Une charte du contrôle sur place, définit le cadre du contrôle sur place ainsi que ses objectifs et obligations réciproques des contrôleurs et des allocataires.

Leurs missions consistent à :

- détecter les mécanismes de fraudes ;
- enquêter, analyser et traiter les fraudes à forts enjeux en coordination avec les contrôleurs des CAF ;
- réaliser et diffuser les modes opératoires et les bonnes pratiques aux CAF.

Par ailleurs, la loi de financement de la sécurité sociale pour 2023³⁹, attribue des pouvoirs d'enquête, notamment de cyber enquête, et des droits de communication de renseignements aux organismes de protection sociale.

Si les résultats de cette disposition ne peuvent pas encore en être mesurés, ces attributions devraient faciliter, par les formations associées à ces missions et les collaborations plus nombreuses avec l'autorité judiciaire qu'elle induit, l'appropriation et le développement de la réponse pénale par les agents des organismes de sécurité sociale. Elle pourrait aussi rendre plus attractifs les postes proposés par le réseau assurance maladie.

3.1.4. Renforcer les échanges d'information avec les autres acteurs publics, notamment pour les processus d'immatriculation et d'identification, contrôle de l'existence et certifications des droits, contrôle de la condition de résidence et de ressources

La CNAM a développé de nombreux partenariats avec les services d'investigations qu'il convient de poursuivre et d'amplifier.

En début de COG 2018-2022, la CNAM contribuait à deux axes du **plan national de coordination de la lutte contre la fraude aux finances publiques 2016-2018** coordonné par la délégation nationale à la lutte contre la fraude (DNLF) :

³⁸ CAF de Seine-et-Marne, de Gironde, du Var, du Nord et du Bas-Rhin ;

³⁹ Article 98.

Annexe III

- ◆ optimiser la gestion de l'information grâce au numérique ;
- ◆ améliorer les techniques d'enquêtes, l'effectivité des sanctions et du recouvrement.

La mission interministérielle de coordination anti-fraude (MICAF), qui a pris la suite de la DNLF en 2020, a une compétence, prévue dans les textes⁴⁰, de coordination et d'impulsion des partenariats interministériels⁴¹, notamment par l'organisation de groupes opérationnels thématiques arbitrés au niveau interministériel, les groupes opérationnels nationaux anti-fraude (GONAF).

La CNAM participe aux groupes suivants :

- ◆ « **Fraude documentaire et à l'identité** » :
 - Dont un protocole signé en 2021 vise à renforcer les échanges d'informations en matière de lutte contre la fraude à l'identité et la fraude documentaire, entre la MICAF, le ministère de l'intérieur et les organismes de protection sociale ;
 - le protocole prévoit la nature des informations échangées par les parties (par exemple les services de police transmettent les listes de faux documents d'identité, de voyages ou de titres de séjour interceptés ; les organismes de protection sociale communiquent chaque année à la MICAF un bilan chiffré et une analyse des fraudes à l'identité sur la base d'une typologie annexée au protocole ;
 - le protocole prévoit aussi un accès par les organismes de protection sociale à différents systèmes d'information : DOCVERIF (application informatique de vérification des titres d'identité), JUSTIF'ADRESSE (pour le contrôle automatisé de la preuve du domicile) et 2D DOC (dispositif de sécurisation des documents). Le protocole prévoit également une offre de formation des agents des organismes de protection sociale à la fraude documentaire et à l'identité ;
- ◆ « **Justice pénale et recouvrement des créances en matière de fraude aux finances publiques** », qui vise à mieux faire partager et interroger les pratiques administratives et judiciaires en vue d'une utilisation plus efficace des voies de droit ;
- ◆ « **Adaptation des moyens d'enquêtes aux enjeux du numérique** » ;
- ◆ « **Fraude à la résidence** » : ce groupe vise à mutualiser les échanges et les contrôles entre organismes de protection sociale pour établir une typologie des fraudes, un référentiel commun de contrôle et des coopérations avec le ministère de l'intérieur ;
- ◆ Des **groupes de travail ponctuels** sont également mis en place par la MICAF sur des thématiques d'actualité à forts enjeux, à l'instar des groupes de travail dédiés aux centres de santé, aux trafics de médicaments onéreux et aux fraudes à enjeux commises notamment par des moyens cyber.

Ces travaux permettent à la CNAM de renforcer les partenariats nécessaires au partage d'information, d'outils et de données, d'accélérer et d'améliorer le traitement pénal des dossiers, notamment dans les affaires complexes dont le traitement judiciaire des contentieux particulièrement lourds a été facilité grâce aux contacts avec les offices centraux, et les parquets via la MICAF, permettant un traitement pénal centralisé.

⁴⁰ Décret no 2020-872 du 15 juillet 2020 relatif à la coordination interministérielle en matière de lutte contre la fraude. Circulaire du Premier Ministre du 27 avril 2021.

⁴¹ Office central de lutte contre les atteintes à l'environnement et à la santé publique –OCLAESP-, office central de lutte contre le travail illégal –OCLTI-, office central de lutte contre la grande répression financière –OCRGDF-, groupes interministériels de recherche –GIR, direction centrale de la police judiciaire –DCPJ-, direction centrale de la police aux frontières –DCPAF-, direction de la coopération internationale de sécurité –DCIS-, préfecture de police, direction des douanes, direction nationale des enquêtes fiscales –DNEF-.

Encadré 4 : La mission interministérielle de coordination anti-fraude (MICAF)

Le nouveau dispositif de coordination interministérielle en matière de lutte contre la fraude aux finances publiques (fraude aux prélèvements obligatoires fiscaux et sociaux, fraude aux prestations sociales) a été institué par un **décret du 15 juillet 2020**, est organisé autour de la **mission interministérielle de coordination anti-fraude (MICAF)**, a pour vocation d'être mieux adapté aux enjeux d'aujourd'hui marqués par des fraudes plus organisées, complexes et mobiles.

Priorité est donnée aux **partages opérationnels de renseignements et à la définition de stratégies communes d'actions entre administrations et organismes partenaires.**

Au niveau national, la MICAF assure à cette fin, en partenariat avec des directions « cheffes de file », un suivi actif de **dix groupes opérationnels nationaux anti-fraude (GONAF)**. Ces groupes réunissent les administrations, les organismes de protection sociale ainsi que les services d'enquêtes administratifs et judiciaires autour des enjeux prioritaires suivants :

- la fraude à la TVA ;
- la contrefaçon ;
- les trafics de tabac ;
- la fraude fiscale et sociale commise via le e-commerce ;
- le travail illégal et la fraude fiscale connexe ;
- les fraudes fiscales et sociales commises via des sociétés éphémères frauduleuses ;
- la fraude à la résidence ;
- la fraude documentaire et à l'identité ;
- l'adaptation des moyens d'enquêtes aux enjeux du numérique ;
- la recherche d'un meilleur recouvrement des créances en matière de fraude aux finances publiques.

Ces GONAF ont pour vocation de favoriser le **décloisonnement des approches par le partage d'informations et d'analyses, l'établissement de cartographies communes des risques**, l'élaboration des stratégies d'actions et d'enquêtes coordonnées. Il s'agit notamment de mieux identifier et combattre les fraudes complexes et organisées en favorisant une meilleure articulation des actions administratives et judiciaires.

Au niveau local, la MICAF assure une coordination des **Comités opérationnels départementaux anti-fraude (CODAF)**, placés sous la coprésidence des préfets et procureurs de la République dans leur forme plénière et, sous la seule présidence des procureurs, dans leur forme restreinte. Leur activité est organisée autour de priorités d'actions et d'échanges de renseignements en matière de fraude aux prélèvements fiscaux et sociaux et de fraude aux prestations sociales. Il s'agit de mobiliser l'ensemble des sanctions administratives et judiciaires en matière de lutte contre la fraude aux finances publiques (redressements, pénalités, récupérations d'indus, sanctions pénales...).

Au niveau européen, la MICAF a également pour vocation institutionnelle de **faciliter la coopération avec les instances européennes** chargées de la protection des intérêts financiers de l'Union européenne et notamment les échanges opérationnels avec l'Office européen de lutte anti-fraude.

Dans ce nouveau cadre interministériel, la MICAF peut impulser de nouvelles synergies en matière d'échanges d'informations entre partenaires, notamment en matière d'interconnexions de données.

3.2. Renforcer l'usage des outils numériques de vérification des droits et poursuivre les chantiers de numérisation des prescriptions

3.2.1. Afin d'éviter le versement de sommes à tort sur la base des droits ouverts en carte, la consultation des droits sur les bases ADRI et CDRI pourrait être rendue systématique par le biais du développement de l'application carte Vitale et d'une obligation conventionnelle

Comme indiqué dans l'annexe I relative à la carte Vitale l'usage des outils ADRI (médecine de ville) et CDRI/CDR est d'ores et déjà largement répandu auprès des professionnels de santé. La consultation de ces bases, directement (CDR) ou par le biais des logiciels métiers des professionnels de santé libéraux (ADRI) ou des établissements de santé (CDRI), permet de consulter et de copier les droits à jours des patients à partir de la base de données patients et d'éviter des facturations erronées.

Néanmoins **la consultation de ces bases n'est ni obligatoire ni systématique**. L'usage de la carte Vitale pour sécuriser le flux SESAM-Vitale permet de bénéficier de la garantie de paiement. Dans le cas où les droits figurants sur la carte Vitale ne seraient pas à jour (fin d'ALD, tiers payant,...), le flux de facturation SESAM Vitale conduira à un rejet in fine par l'organisme d'assurance maladie compétent. **La sécurisation du flux SESAM-Vitale par la carte Vitale emporte une garantie de paiement pour le professionnel de santé** dans le cas où les droits effectifs ne correspondent pas aux droits inscrits en carte.

L'objectif de réduction des paiements effectués par les CPAM au bénéfice des professionnels de santé au titre de la **garantie de paiement pourrait être poursuivi**. La mission n'a pas pu obtenir de données chiffrées nationales concernant le montant total de la garantie de paiement. La CPAM du Rhône a fait état, lors des investigations, d'un montant de garantie de paiement très faible (environ 300 000 €) rapporté à celui des paiements réalisés en 2021 (0,016% des paiements).

Dans le cadre de la lutte contre la fraude, il pourrait être envisagé de renforcer l'usage de ces outils en **prévoyant la consultation systématique des droits des assurés à l'occasion des prestations médicales (cf. annexe IV)**. L'obligation pourrait être établie et associée à la garantie de paiement pour les professionnels de santé ayant correctement effectué la procédure, dans le cas où les droits de l'assuré renseignés par la base ADRI ou CDRI n'auraient pas été corrects.

3.2.2. Tenir le calendrier de déploiement des « ordonnances numériques » prévu jusqu'à fin 2024 pour lutter contre le trafic de médicaments

Service socle du « Ségur du numérique en santé », l'ordonnance numérique (ou « e-prescription ») est déployée au travers d'un nouveau service proposé aux professionnels de santé. L'ordonnance numérique permet de :

- ◆ **sécuriser les prescriptions** en s'assurant que l'ordonnance présentée au professionnel de santé prescrit a bien été établie par un médecin et figure dans la base de donnée dédiée ;
- ◆ **favoriser la coordination des soins** en dématérialisant le circuit de la prescription entre les médecins et les professionnels de santé ;
- ◆ **retrouver les ordonnances au format numérique dans Mon espace santé** (pour le patient), grâce à l'alimentation automatique du DMP à partir du logiciel métier du prescripteur.

Annexe III

Rédigées à partir du logiciel d'aide à la prescription du prescripteur, les **données de la prescription sont automatiquement déversées dans une base de données hébergée en France et sécurisée par l'Assurance Maladie, qui permet au prescrit de les récupérer pour les délivrer ou les exécuter.**

En parallèle, le service permet d'éditer une ordonnance papier remise aux patients contenant toutes les données habituelles, auxquelles s'ajoutent :

- ◆ un **QR code véhiculant un numéro unique de prescription**, permettant d'éviter la fraude aux fausses ordonnances, utilisées à plusieurs reprises ou n'ayant pas été établies par un professionnel de santé ;
- ◆ des mentions légales d'information du patient.

Lorsqu'elle est présentée chez un professionnel prescrit également équipé d'un logiciel référencé Ségur, **l'ordonnance est lue grâce au QR code**. Le professionnel prescrit peut ainsi récupérer directement les informations de prescription alimentées par le prescripteur dans la base de données depuis son logiciel métier. Les **données de délivrance sont également automatiquement enregistrées dans la base de données et peuvent**, avec l'accord du patient (accord recueilli par le prescripteur), **être consultées par le médecin prescripteur**.

Le patient reste libre de choisir le prescrit de son choix. L'ordonnance numérique n'a pas d'impact sur le temps de consultation et préserve la liberté de prescrire.

Toutes les prescriptions effectuées dans le cadre de la médecine libérale sont concernées. Le déploiement se fera progressivement en fonction de l'intégration du service dans les logiciels métiers.

Ce dispositif d'ordonnance numérique est appelé à être généralisé **au plus tard le 31 décembre 2024**⁴². Il se déploie progressivement auprès des différentes catégories de professionnels de santé et pour les différents types de prescriptions :

- ◆ **2022 : début de la généralisation** pour la prescription par les médecins de ville prescripteurs (généralistes et autres spécialistes) des produits de santé (médicaments et dispositifs médicaux) et de tous les autres actes et soins (biologie, actes infirmiers, actes de masso-kinésithérapie, orthophonie, orthoptie et pédicurie) et les pharmaciens ;
- ◆ **2023 : intensification du déploiement de la solution chez les médecins et pharmaciens et déploiement auprès des professionnels de la liste des produits et prestations (LPP) ;**
- ◆ 2024 : déploiement progressif pour l'ensemble des prescrits de ville et application progressive aux actes prescrits en établissements et délivrés en ville.

L'utilisation de ce nouveau service nécessite de disposer d'un **logiciel métier référencé Ségur**. Les médecins bénéficient d'une prise en charge intégrale par les pouvoirs publics de la mise à jour référencée Ségur de leur logiciel de gestion de cabinet.

3.2.3. Compléter la sécurisation des feuilles de soins électroniques, en imposant leur horodatage

Les feuilles de soins électroniques (FSE) constituent un élément central de la sécurisation des flux de remboursement (cf. Annexe I) assurés par les différents régimes d'assurance maladie.

⁴² Ordonnance n° 2020-1408 du 18 novembre 2020 portant mise en œuvre de la prescription électronique.

Annexe III

Afin de limiter les possibilités de fraude des professionnels de santé quant aux cotations de leurs actes, et notamment des actes soumis à majoration car pratiqués la nuit (créneau 20h-minuit ; 6h-8h) ou le dimanche et les jours fériés, les feuilles de soins électroniques pourraient être complétées par un système d'**horodatage, actuellement inexistant. La mention du jour et de l'heure d'édition de la FSE** permettrait un contrôle automatique des incohérences entre les facturations des professionnels de santé et les données temporelles contenues sur la FSE. Actuellement, seul le jour et non l'heure est enregistré par le système.

Par ailleurs la systématisation de la facturation via les téléservices ADRI / CDRI, couplée à un horodatage de ces téléservices, permettrait de détecter les cas de fraude ou de mésusage : en effet, contrairement à la carte Vitale, pour laquelle les soins effectués en journée sont le plus souvent regroupés pour facturation en fin de journée par le professionnel de santé, ces téléservices permettent de facturer « en temps réel », ce qui permettrait de détecter rapidement des comportements atypiques (facturation de plusieurs dizaines de consultations en une seule heure, etc.).

ANNEXE IV

L'application carte Vitale

SOMMAIRE

1. L'APPLICATION CARTE VITALE, QUI AURAIT À TERME VOCATION À ÊTRE MAJORITAIREMENT UTILISÉE PAR LES ASSURÉS, EST UN PROJET QUI VISE, AU-DELÀ DE LA DÉMATÉRIALISATION DE LA CARTE PHYSIQUE, À FOURNIR DES FONCTIONNALITÉS SUPPLÉMENTAIRES ET UN PORTEFEUILLE D'IDENTITÉS NUMÉRIQUES DE SANTÉ	1
1.1. Le projet d'application carte Vitale, lancé en 2016, offre une solution dématérialisée, simplificatrice et innovante, qui s'inscrit utilement dans le cadre d'une dématérialisation plus large des moyens d'identification et du développement des usages du numérique en santé.....	1
1.1.1. <i>Le projet d'ApCV s'inscrit dans le développement des usages numériques publics qui se traduit dans le domaine de la santé par une multiplication des chantiers.....</i>	<i>1</i>
1.1.2. <i>L'équipe projet de l'ApCV, créée en 2016, s'est sensiblement renforcée à partir de 2021 pour porter le développement et les expérimentations de l'application</i>	<i>2</i>
1.2. Si l'ApCV est d'abord une version dématérialisée de la carte Vitale, l'application devrait offrir à terme une panoplie de fonctionnalités complémentaires apportant aux usagers une vraie plus-value.....	3
1.2.1. <i>Si la dématérialisation de la carte Vitale est le premier objectif de l'ApCV, l'application fonctionne également comme une clé d'accès à des services numériques en santé grâce à un portefeuille d'identités.....</i>	<i>3</i>
1.2.2. <i>Le cœur historique du dispositif SESAM Vitale, c'est-à-dire l'appel des droits via ADRI, la facturation des soins et la transmission des flux d'information relatifs aux actes médicaux et pharmaceutiques, constituera en volumétrie l'essentiel des usages de l'ApCV.....</i>	<i>4</i>
1.2.3. <i>Pour l'Assurance maladie, l'application permettra de généraliser progressivement la facturation via le téléservice ADRI, remédiant ainsi à une lacune structurelle majeure de l'architecture locale de la carte actuelle.</i>	<i>5</i>
1.2.4. <i>L'ApCV portera des fonctionnalités plus avancées au-delà de l'usage classique de la carte Vitale, notamment la délégation d'usage de la carte Vitale à un tiers de confiance.....</i>	<i>9</i>
1.2.5. <i>Néanmoins, l'ApCV n'est pas un terminal de consultation des droits et des données de santé.....</i>	<i>11</i>
1.2.6. <i>L'ApCV sera à terme, plus largement, un fournisseur d'identité numérique.....</i>	<i>12</i>
1.2.7. <i>L'ApCV entend répondre aux exigences du règlement de l'UE eIDAS de niveau substantiel</i>	<i>12</i>

1.3.	L'Assurance maladie a l'ambition de développer une application carte Vitale qui serait utilisée à terme par une large majorité des assurés	13
1.4.	À moyen terme, la coexistence prévisible d'un double support de la carte Vitale, sur carte physique et sur smartphone, n'a fait l'objet à ce stade d'aucune réflexion quant à ses conséquences.....	14
2.	DES EXPÉRIMENTATIONS SONT CONDUITES DEPUIS 2019 POUR TESTER LES DÉVELOPPEMENTS ET LES FONCTIONNALITÉS DE L'APCV	15
2.1.	Les expérimentations conduites par le GIE SESAM-Vitale et l'Assurance maladie ont fait l'objet d'un encadrement juridique précis.....	15
2.2.	Une première expérimentation, lancée en septembre 2019, a permis de tester les cas d'usage de l'ApCV mais sur la base du volontariat et d'un champ géographique restreint, ce qui entraîné des tests peu nombreux, réduits à la réalisation de 157 feuilles de soins électroniques	16
2.2.1.	<i>La première expérimentation a été réalisée sur un champ géographique limité, enrôlant uniquement les professionnels de santé volontaires.....</i>	<i>16</i>
2.2.2.	<i>La CNIL approuve le cadre fixé pour la première expérimentation de l'ApCV et, prend notamment acte de l'aspect non obligatoire de l'application carte Vitale et des limitations fixées</i>	<i>18</i>
2.3.	Une seconde phase des expérimentations est conduite depuis septembre 2022 et vise au déploiement d'une application cible intégrant un enrôlement biométrique	20
2.3.1.	<i>La seconde expérimentation à la différence de la première intègre une procédure d'enrôlement biométrique.....</i>	<i>20</i>
2.3.2.	<i>Si la biométrie à l'usage a été écartée après une étude approfondie par l'Assurance maladie et le GIE, un enrôlement biométrique par reconnaissance faciale a été retenue pour permettre une labellisation eIDAS de niveau substantiel.....</i>	<i>20</i>
2.3.3.	<i>La 2^e expérimentation fait également l'objet d'un avis de la CNIL qui rappelle que le recours au SGIN devrait être privilégié pour l'enrôlement sur l'ApCV.....</i>	<i>21</i>
2.3.4.	<i>La procédure d'enrôlement, sécurisée par une validation finale humaine, conformément au référentiel PVID de l'ANSSI, comprend un rapprochement biométrique par algorithme pour authentifier le porteur du smartphone</i>	<i>23</i>
2.3.5.	<i>La présérie initialement testée à partir de septembre 2022 a montré d'importants dysfonctionnements dans la procédure d'enrôlement des assurés</i>	<i>24</i>
2.3.6.	<i>Si une présérie a été déployée au mois de septembre 2022, l'ouverture de la première version cible de l'application au public des huit premiers départements concernés a été décalée de l'automne 2022 au mois de mars 2023</i>	<i>28</i>

2.4. Si les usagers – assurés comme professionnels de santé – sont demandeurs d’une solution dématérialisée, il n’est pas possible au vu de la faible volumétrie des 2 phases de l’expérimentation de conclure positivement à son fonctionnement opérationnel à grande échelle.....	29
3. LA DÉCISION DE GÉNÉRALISER L’APPLICATION CARTE VITALE A DÉJÀ ÉTÉ PRISE AVEC, NÉANMOINS, UN CALENDRIER DE MISE EN ŒUVRE CONNAISSANT UN DÉCALAGE DU FAIT DES DIFFICULTÉS OPÉRATIONNELLES RENCONTRÉES	30
3.1. Sans attendre les résultats des expérimentations conduites, la décision d’une généralisation a été prise et des travaux en ce sens ont été lancés.....	30
3.2. Le calendrier de déploiement a tendance à s’allonger mais demeure ambitieux.....	30
3.3. Plusieurs sujets de fond appellent des réflexions complémentaires.....	32
3.3.1. <i>Le système cible privilégié, à partir du moment où l’application carte Vitale sera largement adoptée par les assurés, reste à déterminer</i>	<i>32</i>
3.3.2. <i>Quand bien même l’ApCV connaîtrait un succès dans son déploiement à terme, le recours via l’application à la biométrie à l’usage n’apportera que de faibles garanties tout en présentant une probable impraticabilité technique</i>	<i>32</i>
3.3.3. <i>L’impact de l’application carte Vitale sur la fraude à l’Assurance maladie devrait être faible</i>	<i>34</i>

Annexe IV

Dans le cadre des travaux sur la fraude aux prestations sociales réalisés entre fin 2019 et début 2021, l'utilisation de la biométrie à chaque utilisation de la carte Vitale avait été proposée par les parlementaires.

Le gouvernement s'est engagé à réaliser une étude de faisabilité sur la carte Vitale sous la forme d'une application smartphone d'e-carte Vitale (ci- après « ApCV » ou « application carte Vitale »). Son expérimentation, avec une phase d'enrôlement ayant recours à la biométrie, est en cours en vue d'un déploiement à plus large échelle.

La présente annexe détaille les objectifs de ce projet d'ApCV, analyse le contexte et les résultats des expérimentations et dresse les perspectives d'articulation de cette application avec les autres projets de l'Assurance maladie et ses développements futurs.

La présente annexe n'aborde pas la question des étrangers en situation irrégulière bénéficiaire de l'aide médicale d'État qui ne disposent pas d'une carte Vitale mais d'une carte d'Aide médicale d'État (AME) avec photographie, dénuée de puce électronique (rapport IGF-IGAS sur l'aide médicale d'État, diagnostics et propositions, d'octobre 2019. Leur nombre était de 318 106 à la fin 2018).

1. L'application carte Vitale, qui aurait à terme vocation à être majoritairement utilisée par les assurés, est un projet qui vise, au-delà de la dématérialisation de la carte physique, à fournir des fonctionnalités supplémentaires et un portefeuille d'identités numériques de santé

1.1. Le projet d'application carte Vitale, lancé en 2016, offre une solution dématérialisée, simplificatrice et innovante, qui s'inscrit utilement dans le cadre d'une dématérialisation plus large des moyens d'identification et du développement des usages du numérique en santé

1.1.1. Le projet d'ApCV s'inscrit dans le développement des usages numériques publics qui se traduit dans le domaine de la santé par une multiplication des chantiers

La feuille de route du numérique en santé présentée fin avril 2019 par le ministère des solidarités et de la santé présente cinq grandes orientations.

La deuxième d'entre elles concerne plus spécifiquement la sécurité et l'interopérabilité des systèmes d'information en santé, qui se traduisent en particulier par :

- ◆ un identifiant national de santé (INS) qui est utilisé comme identifiant de santé des personnes pour leur prise en charge à des fins sanitaires et médico-sociales, sur la base du numéro d'inscription au répertoire national d'identification des personnes physiques (NIR) ; cet identifiant permet le référencement fiable et univoque des données de santé des usagers ; ainsi, seuls les acteurs de la santé et du secteur médico-social concourant à la prise en charge de l'utilisateur et à son suivi, ou menant des actions de prévention, sont tenus d'utiliser l'INS ;
- ◆ l'application carte Vitale ou « ApCV » visant à permettre l'authentification en ligne des assurés maladie ainsi que des utilisations directement auprès des professionnels de santé en remplacement de la carte Vitale ;
- ◆ l'application « e-CPS » permettant l'authentification en ligne des professionnels de santé ainsi que des utilisations en dehors du numérique en remplacement des cartes de professionnel de santé.

Annexe IV

Le système de facturation par la carte Vitale physique est désormais, après plus de 20 ans de développement et d'amélioration, fiabilisé, robuste et présente un coût maîtrisé. Néanmoins, certaines faiblesses intrinsèques à la carte Vitale subsistent. On peut mentionner le fait que beaucoup d'assurés la perdent ou l'oublie, conduisant les professionnels de santé à avoir recours à des feuilles de soin papier. Par ailleurs, les droits inscrits en carte ne correspondent pas toujours aux droits réels (cf. *infra*), lesquels peuvent évoluer sans qu'une mise à jour en temps réel soit opérée sur la puce de la carte Vitale. Enfin, le prêt de carte, qui est une pratique réputée courante, en particulier dans les cadres familiaux, n'est pas encadré, tracé ou suivi.

Un système entièrement dématérialisé est moins coûteux à gérer pour les régimes d'assurance maladie obligatoire qu'un système de cartes physiques. Néanmoins, aucune économie immédiate n'est attendue car le temps du développement et de l'adoption par les assurés de l'application carte Vitale suppose, pour plusieurs années, la coexistence des supports (cf. *infra*). Si à terme le développement de l'ApCV doit aboutir à une réduction du nombre de cartes Vitale physiques en circulation, cela conduira donc à des économies directes sur le coût d'achat, le coût de personnalisation et les coûts de gestion du parc de cartes.

Sur la base de ces réflexions, un projet visant la dématérialisation de la carte Vitale a été progressivement développé avec des objectifs plus larges.

1.1.2. L'équipe projet de l'ApCV, créée en 2016, s'est sensiblement renforcée à partir de 2021 pour porter le développement et les expérimentations de l'application

Les premières réflexions sur la dématérialisation de la carte Vitale remontent à 2012. Fin 2012, le comité directeur du GIE SESAM-Vitale décide en effet d'examiner ce sujet.

A compter de 2016, la Caisse nationale d'Assurance maladie (ci-après « CNAM » ou « Assurance maladie ») et le GIE SESAM-Vitale¹ entament des travaux pour développer une application sur smartphone permettant la déclinaison dématérialisée de la carte Vitale. Les premiers agents engagés dans ces travaux conduisent des études préliminaires d'opportunité et de faisabilité, lançant des discussions avec les industriels sur les aspects techniques qu'une telle solution pourrait présenter. La réflexion a porté également sur les cas d'usage de l'application et sur leur valeur ajoutée par rapport à la carte Vitale physique.

En 2017, une étape est franchie avec la mise à l'épreuve auprès d'assurés et de professionnels d'une maquette de l'application. Le développement de cette maquette a poursuivi deux objectifs :

- ◆ disposer d'un outil de promotion, sous format vidéo, pour montrer aux décideurs publics les cas d'usage, afin de simplifier la communication sur le produit et de rendre réel le sujet ;
- ◆ disposer d'un outil pour lancer un premier test par des utilisateurs. Des panelistes ont été sollicités pour faire réagir un panel de professionnels de santé et d'assurés, à Paris et à Tours sur la maquette et recueillir leurs avis. Des mises en situation ont été organisées pour également permettre aux personnes du panel de réagir en situation. Ces mises en situation ont intégré le cas de la téléconsultation.

Ces travaux ont aiguillé la décision prise en 2018 par le ministère chargé de la Santé et traduite dans la feuille de route du numérique en santé de 2019 de conduire le projet d'une application carte Vitale. À cette fin, l'équipe projet dédiée, mise en place au sein du GIE SESAM-Vitale, a vu ses effectifs croître de manière rapide, comptant 50 ETP en 2021 puis 80 ETP en 2023.

¹ Plus largement, le programme carte Vitale est assuré par un groupement d'intérêt économique, le GIE SESAM-Vitale, créé par la loi n° 93-121 du 27 janvier 1993 portant diverses mesures d'ordre social.

Annexe IV

L'application carte Vitale prendrait la forme d'une application pour téléphone mobile. L'objectif de la CNAM et du GIE SESAM-Vitale est de la rendre accessible à tous les publics et de la rendre disponible sur l'ensemble des plateformes de téléchargement d'applications, c'est-à-dire les stores iPhone OS (iOS) et Android.

Assez tôt dans la conduite du projet, des liens sont établis avec France Connect² et avec le projet France Identité numérique. Dès 2016, des contacts sont établis avec France Connect avec pour objectif initial de permettre, par l'utilisation de l'ApCV d'accéder à France Connect parmi les cas d'usage. Le projet France identité numérique³ est lancé en 2018, avec la nomination d'une cheffe de projet s'appuyant sur une lettre de mission et sur la DINUM. L'équipe du projet application carte Vitale a mis en place dès 2018 des échanges nourris avec le projet France identité numérique, notamment pour déterminer l'articulation future entre une identité numérique sectorielle, en l'occurrence dans le secteur de la santé, et l'identité numérique régaliennne.

Dans la sphère santé, les projets conduits en matière d'identités numériques sectorielles se sont appuyés sur les titres existants, s'agissant tant des assurés (carte Vitale) que des professionnels de santé (CPS). L'idée est d'assurer une transition progressive depuis l'univers de titres physiques existants à la traduction applicative sur smartphone.

1.2. Si l'ApCV est d'abord une version dématérialisée de la carte Vitale, l'application devrait offrir à terme une panoplie de fonctionnalités complémentaires apportant aux usagers une vraie plus-value

1.2.1. Si la dématérialisation de la carte Vitale est le premier objectif de l'ApCV, l'application fonctionne également comme une clé d'accès à des services numériques en santé grâce à un portefeuille d'identités

La carte Vitale a constitué le support matériel d'un programme de dématérialisation des flux de facturation de l'assurance maladie, par la création de feuilles de soins électroniques (FSE).

La carte Vitale a été mise en circulation en 1997. Il lui a été substitué de manière partielle, dix ans plus tard, une version dite « Vitale 2 » comportant une photographie de l'assuré et une puce plus sophistiquée. Les deux générations coexistent aujourd'hui. Outre les feuilles de soins électroniques, la carte Vitale permet à l'assuré d'accéder à son historique de remboursement, à ses arrêts de travail et aux protocoles affections de longue durée (ALD), ainsi que la création et l'alimentation du dossier pharmaceutique.

L'application carte Vitale entend dématérialiser la carte physique tout en procédant à plusieurs enrichissements de l'expérience utilisateur grâce à différents services numériques complémentaires.

L'ApCV se définit en effet comme un dispositif emportant trois fonctions :

² Pour rappel, FranceConnect est la solution de l'État pour faciliter la connexion aux services et démarches en ligne. Il permet d'accéder à plus de 1 400 services en utilisant un compte et un mot de passe que l'utilisateur possède déjà.

³ Le programme interministériel « France identité numérique » (FIN), lancé en 2018, est chargé de concevoir et de mettre en œuvre une solution d'identification numérique pour l'ensemble des citoyens.

Annexe IV

- ◆ une fonction de **carte Vitale digitalisée** qui propose une solution sécurisée et simple d'utilisation pour l'identification, l'authentification et la signature des assurés sur smartphone ; dans cette mesure, l'application porte une identité numérique en santé cohérente avec des usages exclusivement en présence du professionnel de santé ; elle permet également des délégations de droits entre assurés pour une durée maximale de 30 jours ;
- ◆ une fonction de **portefeuille d'identités**, l'application assurant le portage de l'identité d'assuré social par le NIR, de l'identité d'assuré à une complémentaire santé, de l'INS et de traits d'identité civile ;
- ◆ une fonction de **fourniture d'une identité numérique de niveau eIDAS⁴ substantiel** pour l'accès sécurisé des assurés aux services de l'assurance maladie ou de la santé (DMP), notamment dans le cadre de l'espace Numérique de Santé (Mon Espace Santé), où plus largement à des usages du domaine santé/social dans le cadre de l'État-plateforme, c'est-à-dire principalement comme fournisseur d'identité à vocation transversale.

1.2.2. Le cœur historique du dispositif SESAM Vitale, c'est-à-dire l'appel des droits via ADRI, la facturation des soins et la transmission des flux d'information relatifs aux actes médicaux et pharmaceutiques, constituera en volumétrie l'essentiel des usages de l'ApCV

La dématérialisation de la carte Vitale devrait permettre de fournir aux assurés et aux professionnels de santé un moyen d'accès aux mêmes services et usages que la carte physique. Les services de facturation sécurisés, de signature électronique de la feuille de soins et les téléservices de l'Assurance maladie et, pour les pharmaciens, l'accès au dossier pharmaceutique du patient s'appuyant sur la carte Vitale physique seraient d'une manière identique mobilisables par le recours à l'ApCV. Les professionnels de santé comme les assurés y gagneraient en temps et en facilité d'usage.

L'application permet de consulter la situation du patient au regard de ses droits en temps réel par un appel au téléservice Acquisition des DRoits intégrés (ADRI).

Les droits de l'assuré ne sont pas portés par l'application. Celle-ci sert uniquement de clé d'accès au téléservice ADRI (ou CDRi en établissement de santé) préexistant pour connaître en temps réel les droits. Cette architecture permet, dans une logique de développement rapide et de gestion facilitée de l'application, de disposer d'un produit applicatif moins lourd, le rôle de l'application étant donc de pointer vers des services en ligne, en l'occurrence par le biais du numéro d'identification au régime d'assurance maladie obligatoire. Il est néanmoins remarqué qu'ADRI à la différence de la carte Vitale physique n'est pas associée à une garantie de paiement au bénéfice des professionnels de santé pratiquant.

Lors de l'émission d'une feuille de soins, les principales étapes de l'utilisation de l'ApCV sont ainsi les suivantes (cf. Graphique 1) :

- ◆ l'assuré déverrouille au moyen d'un code à 6 chiffres son ApCV et la présente au professionnel de santé ;
- ◆ au moyen d'un équipement dédié, soit par technologie sans contact (« Near field communication » - NFC) soit par lecture d'un code « 2D » (type QR code ou autre), le professionnel de santé accède aux identifiants de l'assuré contenus dans l'application⁵ ;

⁴ Règlement de l'Union européenne n° 910/2014 Electronic IDentification Authentication and trust Services (eIDAS).

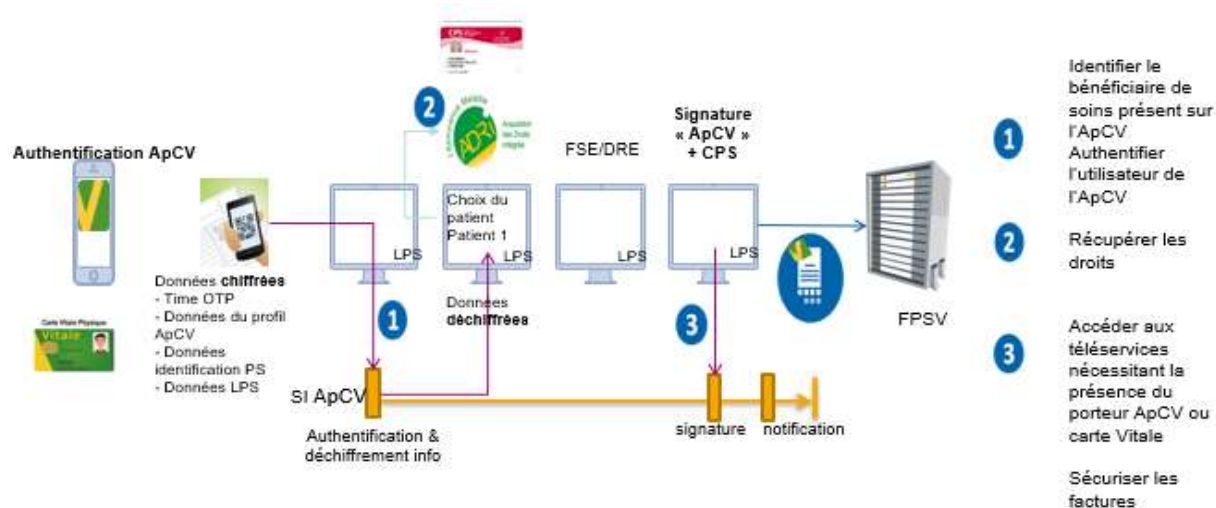
⁵ Les éléments de sécurité dans le QR code sont valables 1 minutes trente secondes avant évolution.

Annexe IV

- ◆ le logiciel-métier du professionnel de santé obtient les droits d'assurance-maladie obligatoire (AMO) de l'assuré par l'intermédiaire du service d'acquisition des droits intégrée (ADRI) ;
- ◆ le professionnel de santé émet une feuille de soins électronique qu'il transmet au serveur de l'Assurance maladie.

Les informations de droits du bénéficiaire de soins retournées par l'AMO se substituent fonctionnellement aux informations de la carte Vitale.

Graphique 1 : Cinématique d'utilisation de l'ApCV pour la facturation SESAM-Vitale chez les professionnels de santé libéraux



Source : CNAM.

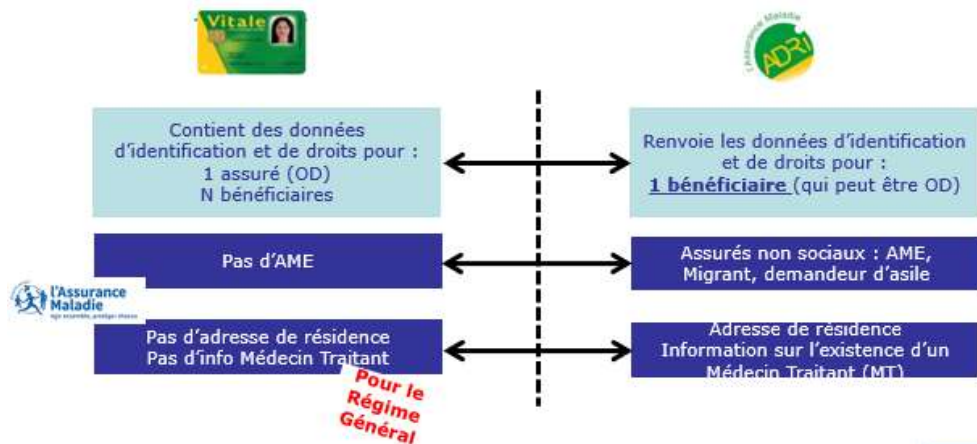
1.2.3. Pour l'Assurance maladie, l'application permettra de généraliser progressivement la facturation via le téléservice ADRI, remédiant ainsi à une lacune structurelle majeure de l'architecture locale de la carte actuelle.

L'application permet, comme mentionnée *supra*, de consulter la situation des droits en temps réel par un appel au téléservice ADRI.

Les données portées par le téléservice ADRI sont aussi plus riches que celles inscrites dans la puce d'une carte Vitale (cf. Graphique 2) avec un envoi des droits des bénéficiaires de l'aide médicale d'État, des migrants et des demandeurs d'asile (non détenteurs de Carte vitale, mais d'une attestation de droits papier) et l'accès à des informations supplémentaires pour les bénéficiaires du régime général (adresse de résidence et de informations sur l'existence d'un médecin traitant).

Annexe IV

Graphique 2 : Comparaison des données contenues dans la carte Vitale et dans le téléservice ADRI

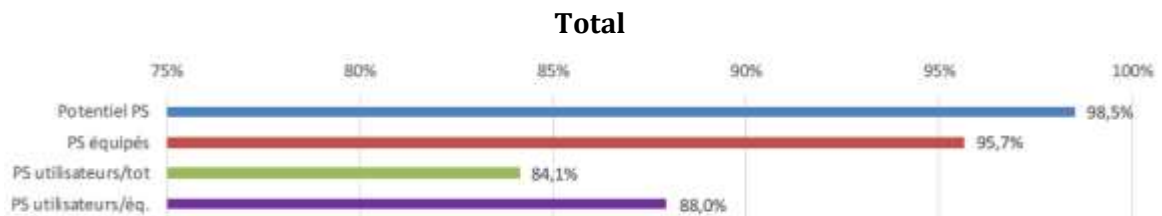


Source : CNAM.

À fin novembre 2022, 88 % des logiciels du marché sont agréés ADRI. 388 279 professionnels de santé en sont équipés soit 95,6 % du total et **88,0 % des professionnels équipés l'utilisent chaque mois, à hauteur de 65 millions d'appels ADRI mensuels.**

La fréquence de ces appels est paramétrable dans les solutions logicielles, en mode ciblé (déclenchement systématique en cas d'absence de carte Vitale, en cas de carte Vitale non à jour, ou en situation de tiers-payant réglementaire), en mode systématique (déclenchement automatique), ou en mode manuel⁶.

Graphique 3 : Situation du déploiement du téléservice ADRI chez les professionnels de santé à fin novembre 2022⁷



Source : CNAM, Tableau de bord ADRI novembre 2022.

Le recours au téléservice ADRI (et au téléservice équivalent « CDRI » dans les établissements de santé) constitue une avancée par rapport à l'utilisation classique de la carte Vitale physique par les professionnels de santé.

Actuellement, les informations relatives aux droits en matière de prise en charge des frais de santé sont stockées dans la puce de la carte physique, et devraient idéalement être mises à jour régulièrement, à l'initiative de l'assuré, lorsque sa situation a changé comme par exemple en cas de changement de régime, de rattachement ou détachement d'un ayant-droit.

⁶ Source : CNAM DDGOS.

⁷ 'Potentiel PS' indique la part des professionnels de santé dont l'éditeur a une offre ADRI ; 'PS équipés' indique la part des professionnels de santé équipés d'un logiciel ADRI ; 'PS utilisateurs / tot' indique la part des professionnels de santé utilisateurs d'ADRI au cours du mois écoulé sur le total des professionnels de santé (équipés ou non) ; le taux 'PS utilisateurs / eq' donne la part des utilisateurs effectifs sur le total des professionnels de santé équipés.

Annexe IV

En pratique, cette opération est effectuée en moyenne 1,2 fois par an – le plus souvent à l'initiative des pharmaciens⁸, mais 6 millions de cartes (soit environ 10 % du parc) ne sont pas mises à jour, ne serait-ce qu'une seule fois par an⁹. Les droits ainsi contenus en carte ne sont donc pas nécessairement à jour lorsqu'il en fait la présentation au professionnel de santé pour la facturation d'un acte.

Or, que les droits en carte aient été ou non actualisés, les professionnels de santé bénéficient d'**une garantie de paiement des droits inscrits sur la puce**. En effet, si un assuré utilise par exemple une carte Vitale présentant en carte des droits, alors que cette personne a vu ses droits fermés, dans le cas d'un tiers payant intégral et de la garantie de paiement, la personne n'a rien à déboursier et le professionnel de santé est remboursé. Le régime d'assurance maladie doit donc supporter un préjudice financier. Cette situation entraîne des indus dont le montant n'a pas pu être évalué précisément.

L'application carte Vitale permet au contraire de s'assurer, sous réserve de la disponibilité du téléservice ADRI (cf. Encadré 1), de disposer des droits à jour de l'assuré et ainsi d'**éviter toute erreur dans la facturation établie** car l'application conduit à un appel aux droits en ligne renseignés dans les bases de l'assurance maladie obligatoire. Au vu des sommes potentiellement en jeu, cette mise en cohérence en temps réel représente un réel atout en corrigeant une faiblesse majeure du système d'information actuel.

Le taux de FSE réalisé avec ADRI s'établissait à 24,7 % en moyenne en 2022, soit un quart du nombre total des FSE annuelles émises¹⁰.

⁸ Qui disposent du matériel nécessaire en lecture / écriture pour modifier les données stockées sur la carte Vitale, contrairement aux autres professionnels de santé (sauf exceptions).

⁹ Source : SESAM Vitale.

¹⁰ CNAM. Données établies à partir des données figurant dans le tableau de bord de novembre 2022. Q01-T04-01-Tableau_de_bord_de_suivi_ADRI_novembre_2022.pdf

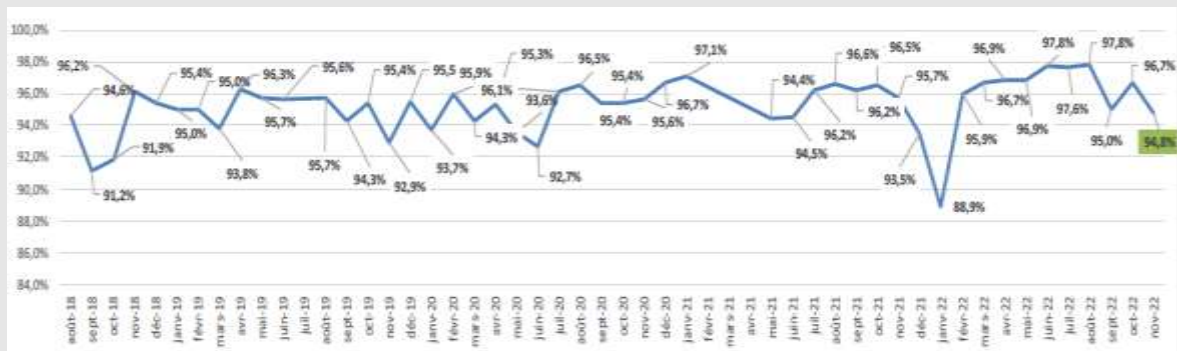
Encadré 1 : La disponibilité du téléservice ADRI

Le téléservice ADRI (Acquisition des droits intégrée) permet, en temps réel, de consulter les droits d'un assuré social, quel que soit son régime d'appartenance. Ce téléservice est intégré au sein des solutions logicielles des professionnels de santé, qui peuvent consulter, sur la base du NIR du patient, l'étendue de ses droits.

En théorie, les droits affichés par ADRI sont de la même nature que ceux inscrits sur la carte Vitale. Ainsi, si la mention d'une ALD est bien présente sur ADRI, sa nature n'est pas précisée et le professionnel de santé devra consulter le portail Ameli-pro afin de la connaître.

Deux difficultés viennent toutefois entraver le bon fonctionnement de ce service :

- bien que le taux de disponibilité¹¹ du téléservice ADRI soit globalement très bon, il varie selon les mois entre 94 % et 98 %¹² comme le montre le graphique ci-dessous présentant l'évolution de la qualité de service du téléservice ADRI sur la période 2018-2022 :



Source : CNAM /DDGOS / tableau de bord ADRI novembre 2022.

- en octobre 2022, 3,5 % des requêtes avaient échoué sans qu'une anomalie expliquant cet échec – par exemple l'assuré n'existe pas en base – soit identifiée (ce taux dépassant 90% s'agissant des anciens ressortissants du RSI). L'Assurance maladie considère que la qualité de service pourrait être fiabilisée par des travaux sur l'infrastructure et par la mise en place d'outil de supervision pour la détection de panne, ou prédictions de pannes".
- le flux des données transmises en retour aux professionnels de santé ne permet pas de gérer certaines situations, ce qui pose notamment problème aux pharmaciens. À titre d'illustration, à l'occasion de la réunion de la commission paritaire locale de Saône et Loire du 24 mars 2022, la section professionnelle des pharmaciens relève « qu'ADRI ne permet pas de gérer deux exonérations », générant ainsi des rejets. Dans le même cadre mais dans la Côte d'Or, un membre la section professionnelle indiquait, lors de sa réunion du 17 octobre 2022, que « lorsque l'assuré est en invalidité et en ALD, ADRI ne gère que l'ALD. Pour les soins hors ALD, le pharmacien facture alors avec application du ticket modérateur. Or, la facture est rejetée car elle aurait dû être facturée à 100 % au titre de l'invalidité ».

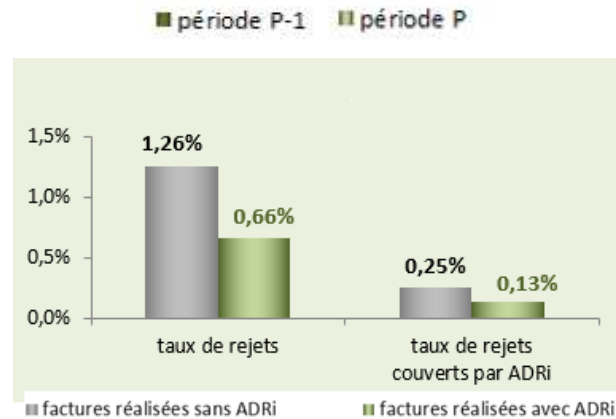
Les éléments communiqués par l'Assurance maladie confirment que **le recours au téléservice permet de réduire sensiblement le taux de rejet, tous flux de facturation confondus (dégradés, non dégradés), et en particulier de diviser par 2 le taux de rejet des factures réalisées avec une carte Vitale** (cf. Graphique 4). Le « taux de rejets couverts par ADRI » indique la part des rejets issus de la comparaison avec la base des droits ouverts (BDO).

¹¹ La disponibilité du système d'information correspond au taux de réussite des appels au téléservice.

¹² CNAM, DDGOS, taux entre août 2018 et novembre 2022.

Annexe IV

Graphique 4 : Comparaison des taux de rejet des flux sécurisés avec carte SESAM-Vitale avec ou sans ADRI au 3^{ème} trimestre 2022 (flux B2S)



Source : Assurance maladie, LDC 2018-001 v2 – Étude impact ADRI rejets liés aux droits – CRF v18.

L'apport serait particulièrement net s'agissant de la sécurisation de l'ouverture des droits aux assurés, dont un grand nombre de bénéficiaires présentent une carte Vitale mais s'avèrent inconnus ou absents de la base des droits ouverts (cf. Tableau 1). Si on projette le nombre de rejets de facturation qui pourraient être évités annuellement avec un recours systématique à ADRI, uniquement à partir de ces 5 principales anomalies, ce sont 2 815 036 cas de rejets qui pourraient être évités chaque année (dont 1,4 million pour bénéficiaire absent ou assuré inconnu de la base des droits ouverts).

Tableau 1 : Liste des 5 premières anomalies constatées avec ou sans utilisation d'ADRI en nombre, tous flux de facturation confondus (B2S/B2F/B2D), au 3^{ème} trimestre 2022

Libellé anomalie ayant entraîné un rejet	Nombre de factures émises	
	Avec utilisation ADRI	Sans utilisation ADRI
Contrat CMU-C ou ACS transmis différent de celui présent au référentiel	110 329	247 831
Bénéficiaire inconnu dans la base des droits ouverts	778	177 750
Assuré absent de la base de droits ouverts	2 142	172 736
Le régime transmis est différent de celui présent dans les fichiers de l'Assurance maladie	18 347	120 063
L'exonération est sur la carte vitale mais n'est pas trouvée dans le fichier à la date des soins	6 211	123 186

Source : CNAM, LDC 2018-001 v2 - Étude impact ADRI rejets liés aux droits - CRF v18.

En conclusion, **l'application carte Vitale, par l'appel de téléservices, devrait permettre aux régimes d'assurance maladie d'éviter certains préjudices financiers constatés dans les cas d'utilisation de cartes Vitale non à jour.**

1.2.4. L'ApCV portera des fonctionnalités plus avancées au-delà de l'usage classique de la carte Vitale, notamment la délégation d'usage de la carte Vitale à un tiers de confiance

Au-delà de la dématérialisation des fonctionnalités de la carte Vitale physique et de la plus grande exactitude des droits intégrés à la facturation, l'ApCV les prolongera par :

- ◆ une facturation d'actes médicaux dans les situations de mobilité des professionnels de santé et de téléconsultation ;

Annexe IV

- ◆ une meilleure visibilité des professionnels de santé aux données médicales et de facturation (transmission plus fluide des identifiants AMO et AMC) ;
- ◆ une délégation à un tiers rendue possible et qui serait encadrée.

1.2.4.1. La capacité nouvelle de procéder à des facturations sécurisées et bénéficiant de la garantie de paiement d'actes de téléconsultation répond à un angle mort actuel de la facturation

Avec l'ApCV, les flux de facturation des téléconsultations seraient sécurisés au niveau des autres flux actuels SESAM-Vitale, bénéficiant d'une double signature électronique.

Actuellement, si le patient est connu du médecin téléconsultant, le médecin dispose déjà des données administratives nécessaires à la facturation. Si le patient n'est pas connu du médecin téléconsultant, les données administratives nécessaires à la facturation sont recueillies par appel à ADRI. Le médecin téléconsultant dont le logiciel métier intègre les fonctionnalités prévues par l'avenant 18 « télémédecine » au cahier des charges SESAM Vitale transmet une feuille de soins électronique en mode SESAM sans Vitale, en l'absence de carte Vitale du patient. Le médecin téléconsultant dont le logiciel métier n'est pas à jour conformément à l'avenant 18 « télémédecine » au cahier des charges SESAM Vitale transmet en mode SESAM dégradé. À titre dérogatoire, le médecin est exonéré, dans ce cas, de l'envoi de la feuille de soins papier parallèlement au flux télétransmis.

1.2.4.2. Dans le champ des établissements de santé, l'ApCV, application portant au nombre des différentes identités de l'assuré social notamment l'INS s'intégrera aux efforts de dématérialisation et de simplification du parcours de soin

L'application permettra de :

- ◆ réaliser les préadmissions sur des portails en ligne mis à la disposition des patients pour organiser leur future admission, transmettre les pièces justificatives de leur situation, en vue d'une prise en charge pour des soins programmés ;
- ◆ d'automatiser davantage la phase d'accueil physique, par exemple par une orientation vers de bornes d'enregistrement auprès desquels les patients se feront connaître ;
- ◆ faciliter et fluidifier les opérations d'identification conduites par les agents des services d'admission qui pourront utiliser les différentes identités en portefeuille dans l'application, dont l'INS qui est utilisé pour le référencement des données de santé¹³.

Il est à noter que le référentiel INS liste les dispositifs éligibles pour mettre à disposition des personnels soignants un INS qualifié. L'enjeu pour l'ApCV à terme, après certification par l'ANSSI, est de figurer dans cette liste afin de pouvoir être en usage auprès des professionnels de santé comme un outil validé dans la procédure d'identitovigilance.

¹³ Décret n° 2019-1036, relatif au référencement des données de santé avec l'INS.

1.2.4.3. La gestion des délégations représente une autre fonctionnalité de l'ApCV, qui constitue une plus-value majeure par rapport au système actuel qui ne la prévoit pas

Le prêt d'une carte Vitale de son titulaire à un tiers s'avère être une pratique justifiée et généralisée dans un certain nombre de cas, par exemple pour permettre la délivrance de médicaments à une personne malade dans l'incapacité de se déplacer à l'officine, ou pour la délivrance de soins à un enfant placé sous la responsabilité de membres de sa famille non dépositaires de l'autorité parentale (par exemple pendant les vacances scolaires notamment). Ce cas d'usage répond à un besoin courant mais n'est actuellement encadré par aucun texte ni dispositif technique de sécurisation. En particulier, le consentement du délégataire ne peut, dans l'état actuel, être ni établi, ni garanti, ni retiré. Cette pratique est donc tolérée, mais ne constitue pas une situation satisfaisante.

Le mécanisme de délégation prévu dans le cadre de l'ApCV consiste en la transmission des données d'identification à un tiers, sans perte du bénéfice du dispositif pour l'assuré délégant. Outre les cas d'usage mentionnés, les majeurs protégés (tutelle et curatelle) pourront également bénéficier de ce service. Ces délégations pourront être consenties à distance ou en proximité, selon des modalités optimisant l'expérience utilisateur.

Les principaux axes de sécurisation de la délégation par l'ApCV sont les suivants :

- ◆ limitation de la durée, librement définie par le délégant pour une durée pouvant aller jusqu'à 30 jours ;
- ◆ exclusivité du prêt ;
- ◆ révocabilité de la délégation, tant pour le délégant (prêteur) que pour le délégataire (receveur) ;
- ◆ traçabilité de l'utilisation des délégations dans le système d'information de l'assurance-maladie, tendant à en encadrer l'usage.

La délégation à un tiers a été incluse dans la première expérimentation, conduite à partir de 2019. Elle n'a en revanche pas été prévue dans la phase de déploiement, engagée par une présérie à compter de l'automne 2022 puis élargie en 2023. En effet, lors de l'expérimentation, seuls les agents des CPAM avaient testé cette fonctionnalité, ce qui a permis d'alimenter l'avant-projet en cours pour l'application cible. Mais des compromis techniques ont été faits sur la sécurité et la traçabilité, qui ne peuvent être retenus pour un déploiement à grande échelle. Cette fonctionnalité ne serait donc développée et intégrée à l'application qu'après sa généralisation, soit fin 2024 ou plus probablement en 2025.

1.2.5. Néanmoins, l'ApCV n'est pas un terminal de consultation des droits et des données de santé

L'application ne permettra pas, notamment :

- ◆ une visualisation, un stockage ou une transmission des données de santé, y compris celles contenues dans le dossier médical partagé (DMP) ;
- ◆ une consultation des droits ou des prescriptions.

L'application carte Vitale, en revanche, permettra de consulter ses usages par un résumé des dépenses de soins rappelant l'identité du professionnel de santé et le montant associé.

1.2.6. L'ApCV sera à terme, plus largement, un fournisseur d'identité numérique

L'assuré disposerait via l'ApCV d'une identification numérique lui permettant de s'authentifier sur des services numériques du secteur santé-social et notamment sur 'Mon espace santé'.

La doctrine du numérique en santé détermine pour le domaine médical et de la santé des supports d'identification de référence qui sont positionnés au même rang que France Connect. D'après la doctrine, compte tenu de la sensibilité des données médicales manipulées, les conditions d'accès et le référentiel européen de sécurité doivent présenter une certaine force, dans la logique du référentiel sur l'identification électronique et les services de confiance pour les transactions électroniques, dit règlement Electronic IDentification Authentication and trust Services (eIDAS), qui positionne des niveaux de sensibilité des services et des niveaux de robustesse et les met en regard pour déterminer des équivalences.

Dès que le développement du service de l'identité numérique attaché à l'ApCV sera prêt pour l'intégration aux cas d'usage de l'application, l'intégration à « France connect » sera opérée après qualification eIDAS par l'ANSSI.

1.2.7. L'ApCV entend répondre aux exigences du règlement de l'UE eIDAS de niveau substantiel

L'application carte Vitale devra répondre aux normes édictées par le règlement de l'UE sur l'identification électronique et les services de confiance pour les transactions électroniques (règlement Electronic IDentification Authentication and trust Services - eIDAS).

Aux termes de l'article 3 du règlement n° 910/2014 eIDAS, les schémas d'identification électronique font référence aux « *processus consistant à utiliser des données d'identification personnelle sous une forme électronique représentant de manière univoque une personne physique ou morale, ou une personne physique représentant une personne morale* ».

L'application carte Vitale ayant pour objectif d'être labélisée eIDAS au niveau substantiel, les solutions d'identification qui seront étudiées devront respecter les contraintes associées à cette labélisation et ne pas induire de risque vis-à-vis de cet objectif stratégique.

Le règlement eIDAS a établi trois niveaux de garantie des schémas d'identification électronique – Faible, Substantielle et Élevée – qui accordent des degrés correspondant de fiabilité à l'identité revendiquée ou prétendue d'une personne.

Pour revendiquer un niveau de garantie donné, un schéma d'identification doit vérifier les exigences fixées par le règlement (cf. Tableau 2), relatives aux quatre thématiques suivantes :

- ◆ le processus d'enrôlement du schéma ;
- ◆ la force de son authentification ;
- ◆ la conformité ISO 27001 de son système de gestion ;
- ◆ ses procédures organisationnelles.

Une application carte Vitale doit donc être conforme aux exigences de niveau substantiel sur ces quatre thématiques dès lors qu'elle se positionne comme solution d'identification au sens du règlement eIDAS.

Le choix n'a pas porté sur une labellisation de niveau élevé qui ne correspondait pas aux objectifs premiers poursuivis par le développement de l'application et qui emportait trop de contraintes par rapport aux finalités du dispositif.

Tableau 2 : Exigence du règlement eIDAS pour un niveau de garantie substantielle

Thématique	Principales exigences supplémentaires pour le niveau substantiel par rapport au niveau faible
Processus d'enrôlement du schéma	Vérification d'authenticité des documents d'identité physiques à distance <ul style="list-style-type: none"> - Utilisation du référentiel PRADO - Détection de documents falsifiés ou contrefaits Vérification de l'identité d'une personne physique à distance <ul style="list-style-type: none"> - Résistance face aux manipulations d'images et de vidéos, des canaux de communication, et de l'environnement (ex. port de masque) - Utilisation de technologies de détection du vivant
Force d'authentification	Conception et délivrance <ul style="list-style-type: none"> - Utilisation de 2 facteurs d'authentification de différentes catégories - Qualification élémentaire du dispositif : CSPN requise Authentification et appairage du dispositif <ul style="list-style-type: none"> - Authentification dynamique (OTP, challenge-réponse, etc.) - Qualification élémentaire du dispositif : CSPN requise
Conformité et audit	Audit PASSI ou ISO 27001 Audit de la solution de vérification d'identité à distance par un CESTI
Système de gestion et procédures organisationnelles	Adhérence du système de gestion de la sécurité de l'information à des normes ou principes éprouvés pour la gestion et le contrôle des risques de sécurité de l'information Protection contre toute manipulation non autorisée des matériels cryptographiques sensibles utilisés pour la délivrance des supports d'identités

Source : CNAM.

1.3. L'Assurance maladie a l'ambition de développer une application carte Vitale qui serait utilisée à terme par une large majorité des assurés

En France, 75 % des adultes possèdent un smartphone¹⁴ en 2018. L'enquête Baromètre 2022 du numérique estimait, sur la base des réponses obtenues des internautes enquêtés, que le taux d'équipement en smartphone atteignait mi-2022 87 %¹⁵.

Toutefois, seule une partie du parc sera *in fine* dotée à terme de l'application carte Vitale :

- ◆ la totalité de la population n'utilisant pas de smartphones ou de smartphones compatibles ;

¹⁴ Étude sur le Numérique 2018

¹⁵ En dessous de 70 ans, la part des internautes chez les enquêtés dépasse 96% dans chaque catégorie d'âge. Pour les plus de 70 ans, ce taux n'en est pas moins conséquent, avec 63% ; source : [Baromètre du numérique, les chiffres clés 2022](#).

Annexe IV

- ◆ le téléchargement de l'application repose sur une base volontaire des assurés, qui peuvent choisir de ne pas télécharger l'application soit parce qu'ils ne sont pas familiers avec la technologie des smartphones, soit parce qu'ils préfèrent le support physique (carte) ou papier.

L'application carte Vitale ne pourra donc pas constituer le seul support des droits en dehors de l'attestation papier, à tout le moins à court et moyen terme.

L'Assurance Maladie et le GIE SESAM-Vitale estiment que le potentiel total de bénéficiaires qui pourraient être équipés d'une application carte Vitale est d'environ 42 millions. En comparaison il y a 58 millions d'assurés équipés d'une carte Vitale. Le taux de couverture de la population porteuse d'une carte Vitale valide par l'application pourrait donc être d'environ 72,4 %.

1.4. À moyen terme, la coexistence prévisible d'un double support de la carte Vitale, sur carte physique et sur smartphone, n'a fait l'objet à ce stade d'aucune réflexion quant à ses conséquences

Le schéma général d'articulation future des différents supports des droits aux prestations d'assurance maladie n'est pas déterminé à date.

La CNAM et le GIE SESAM-Vitale conduisent le développement de l'application carte Vitale en parallèle de la carte Vitale physique dans une logique similaire à celle déployée aujourd'hui par les banques dans l'utilisation de la carte bancaire, associant concomitamment un support physique et un support dématérialisé.

Dans le cas de l'application carte Vitale, l'Assurance maladie comme les professionnels de santé et leurs représentations rappellent qu'une bascule totale vers une solution dématérialisée risquerait d'entraîner une rupture dans l'accès aux soins et l'exercice des droits des assurés. Les personnes âgées et vulnérables sont celles qui consomment le plus de soins et qui sont également le plus éloignées du numérique (cf. *supra*). L'acquisition d'un smartphone ou sa maîtrise ne sont pas des capacités universelles. Considérant ainsi le risque posé par la fracture numérique, la dématérialisation intégrale n'est pas recherchée à ce stade.

En outre, une partie de la population préfère utiliser les supports physiques (carte, papier...) que de recourir aux applicatifs dématérialisés, comme en atteste l'exemple de la Principauté de Monaco, où 40% des résidents continuent d'utiliser leur carte de santé physique alors que la bascule vers l'application mobile a été opérée et généralisée (bien que récemment).

Pour autant, les différentes parties prenantes du projet d'application carte Vitale voient dans son développement l'opportunité à terme d'avoir à gérer moins de cas de cartes perdues, oubliées et donc moins de flux dégradés. À l'hôpital, l'application carte Vitale aurait pour objectif de s'insérer dans les développements récents d'un parcours d'admission de plus en plus dématérialisé. Le développement d'une solution de carte Vitale dématérialisée, offrant un lien vers l'INS qualifié, pour de nombreux assurés devrait se traduire par un amenuisement plus conséquent encore de la place qu'occupe aujourd'hui la carte Vitale physique dans les établissements de santé. Les parcours usagers en seront facilités.

La migration progressive des usages est jugée longue. Aucun jalon temporel n'est établi, ni aucun objectif en termes de nombre d' enrôlement ou d'utilisation. Pour un temps, l'Assurance maladie estime que, du fait de la séparation du système informatique de l'ApCV et de celui de la carte vitale physique, une part importante des professionnels de santé ne seront pas équipés de lecteur pour lire l'application. Tous les professionnels de santé n'acceptant pas l'application carte Vitale, les usagers seront en retour contraints de présenter leur carte physique ou une attestation de droits papier.

Si à long terme, la CNAM reconnaît un but de réduction du nombre de cartes physiques, cet objectif n'a pas encore fait l'objet de travaux de réflexion, la priorité immédiate étant portée au développement et au succès du lancement de l'application carte Vitale.

2. Des expérimentations sont conduites depuis 2019 pour tester les développements et les fonctionnalités de l'ApCV

2.1. Les expérimentations conduites par le GIE SESAM-Vitale et l'Assurance maladie ont fait l'objet d'un encadrement juridique précis

Un cadre réglementaire a structuré les expérimentations conduites depuis 2019. La délivrance, le déploiement et les usages de l'application carte Vitale ont été encadrés par :

- ◆ le décret n° 2019-528 du 27 mai 2019 relatif à l'expérimentation d'une «e-carte d'assurance maladie»
- ◆ le décret n° 2020-1250 du 13 octobre 2020 prorogeant l'expérimentation d'une «e-carte d'assurance maladie»
- ◆ le décret n° 2021-1014 du 30 juillet 2021 prorogeant et étendant l'expérimentation d'une « e-carte d'assurance maladie »

La généralisation du déploiement de l'application carte Vitale est encadrée par l'ordonnance n° 2021-581 du 12 mai 2021 relative à l'identification électronique des utilisateurs de services numériques en santé et des bénéficiaires de l'assurance maladie et ses textes d'application.

Plus particulièrement, les contrôles biométriques réalisés à l'enrôlement dans les expérimentations conduites sur l'application carte Vitale sont encadrés par la réglementation relative à la protection des données personnelles et donc par les textes suivants :

- ◆ l'article 32 de la Loi Informatique et Libertés du 6 janvier 1978 (modifiée par l'ordonnance n°2018-1125 du 12 décembre 2018) permet, sur autorisation par décret en Conseil d'État, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés (CNIL), les traitements de données à caractère personnel mis en œuvre pour le compte de l'État, agissant dans l'exercice de ses prérogatives de puissance publique, qui portent sur des données génétiques ou sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes ;
- ◆ l'article 9 du règlement général sur la protection des données de l'Union européenne (RGPD), dans son alinéa 2b définit une exception à l'interdiction de traitement au titre de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement en matière de sécurité sociale et de protection sociale, dans la mesure où ce traitement est autorisé par le droit d'un État membre qui prévoit des garanties appropriées pour les droits fondamentaux et les intérêts de la personne concernée.

La CNIL a particulièrement rappelé qu'il convient de raisonner par cas d'usage en fonction de la technologie utilisée avec notamment l'objectif d'évaluer les risques pour les personnes ; toute violation de données, tout mésusage ferait peser des risques importants (blocage d'accès à un service, usurpation d'identité, etc.). Elle rappelle également que le fournisseur d'une application ou d'un service recourant au dispositif biométrique du smartphone est responsable du traitement mis en œuvre par son application et notamment de la sécurité de son application.

Ainsi, le recours aux dispositifs biométriques peut être justifié au regard de l'impératif de forte fiabilité de vérification d'identité, impératif que le projet d'application carte Vitale a intégré.

Cette mise en œuvre doit cependant se conformer à un ensemble de recommandations des institutions indépendantes :

Annexe IV

- ◆ le respect des obligations prévues par le RGPD et en particulier la réalisation d'une Analyse d'impact relative à la Protection des Données ou AIPD (cette analyse est déjà prévue dans le cadre plus global de l'application carte Vitale) ;
- ◆ le respect du droit des personnes, il s'agira en particulier d'informer et de garantir le contrôle de leurs données (maîtrise du gabarit par la personne concernée). Une attention doit être portée sur la protection particulière dont doivent bénéficier les enfants.

Outre le respect de la réglementation relative à la protection des données personnelles et de la doctrine de l'autorité de contrôle, l'usage de la biométrie nécessite une attention particulière relative au respect des droits des personnes et droits fondamentaux.

Afin de s'assurer du respect de ces droits, des recommandations à destination des autorités publiques sont émises visant à :

- ◆ mettre en place des garanties fortes et effectives pour s'assurer du respect des droits des individus ;
- ◆ s'interroger systématiquement sur l'opportunité d'utiliser une technologie moins intrusive, contrôler systématiquement les biais discriminatoires et faciliter le droit au recours ;
- ◆ repenser les contrôles existants, notamment :
 - intégrer les enjeux de risques discriminatoires aux analyses d'impact relatives à la protection des données imposées par l'article 35 du RGPD ;
 - intégrer une appréciation des risques de discrimination et en instaurant une obligation de recourir à un audit régulier, externe et indépendant des dispositifs biométriques d'identification et d'évaluation.

2.2. Une première expérimentation, lancée en septembre 2019, a permis de tester les cas d'usage de l'ApCV mais sur la base du volontariat et d'un champ géographique restreint, ce qui entraîné des tests peu nombreux, réduits à la réalisation de 157 feuilles de soins électroniques

2.2.1. La première expérimentation a été réalisée sur un champ géographique limité, enrôlant uniquement les professionnels de santé volontaires

Une première expérimentation a été lancée en septembre 2019 afin d'observer l'utilisation de l'application carte Vitale dans la vie de tous les jours (facilité de l'installation sur le smartphone et de la prise en main, ergonomie, cas réels d'usage, pertinence des technologies mises en œuvre, identification des freins).

Le champ géographique de cette expérimentation a été très restreint. Seuls 2 organismes du régime général (CPAM Rhône et CPAM Alpes-Maritimes) et 2 organismes de la MSA (Ain-Rhône et Provence-Azur) ont été intégrés à l'expérimentation.

Dans ces départements, seuls les professionnels de santé volontaires - médecins, pharmaciens, infirmiers, kinésithérapeutes, opticiens et centres de santé - rattachés à ces 4 organismes ont fait partie de cette première expérimentation. Les éditeurs, partenaires de l'expérimentation, les ont équipés au préalable d'une solution informatique compatible (NFC sans contact ou QR code) pour l'échange des informations entre le smartphone de l'assuré et le logiciel du professionnel : seules quelques solutions logicielles ne pouvaient y participer. À fin mars 2022, 7 éditeurs de logiciels participaient à l'expérimentation alors que 23 étaient volontaires.

Des assurés faisant partie de la patientèle de ces professionnels de santé ont été invités par courriel par la caisse primaire d'Assurance maladie ou par la MSA à installer et tester l'application carte Vitale sur leur smartphone.

Annexe IV

Ces premiers flux ont été catégorisés comme des flux SESAM sans Vitale, donc non sécurisés totalement, à la différence des flux de la seconde expérimentation, considérés comme des flux SESAM Vitale, bénéficiant donc du niveau le plus élevé de sécurité des flux de facturation.

Le processus d'enrôlement de cette première expérimentation s'appuyait sur une vérification d'identité à distance sans inclure de traitement biométrique. L'assuré devait envoyer des photographies de sa pièce d'identité et de son visage, sans mise en place d'un flux vidéo. Les captures d'images fixes ont fait ensuite l'objet d'une vérification de conformité avant activation par les agents des CPAM participantes.

À la fin du mois d'août 2022, cette expérimentation comptabilisait **114 professionnels de santé équipés** (22 médecins, 48 pharmaciens, 9 opticiens et 44 infirmiers). **Le test n'a pas été réalisé en établissement de santé.** Du côté des utilisateurs, **6 430 assurés avaient activé l'application carte Vitale sur leur smartphone.** Cette population d'assurés et de professionnels de santé, par définition, était composée de personnes motivées pour participer à l'expérimentation, familières ou présentant donc probablement un intérêt pour les nouvelles technologies. Elles pouvaient bénéficier d'un accompagnement personnalisé dans leur démarche, ce qui est un autre facteur de différenciation par rapport à une utilisation d'une application en condition réelle.

Au cours de cette expérimentation, **seules 157 feuilles de soin électroniques ont été établies**, dont plus de 100 auprès des pharmaciens, soit plus de 64 %. Le bilan communiqué à la mission ne précise pas si la réalisation d'une feuille de soins à partir de l'appli s'est concrétisée pour tous les professionnels engagés, ou au moins une fois pour toutes les catégories, ou si elle s'est cantonnée à une poignée d'individus.

Le nombre limité d'assurés et de professionnels de santé ayant testé l'application est d'abord dû à un ciblage serré des expérimentateurs et à la crise sanitaire de 2020 qui a contraint à une suspension de l'expérimentation de la mi-mars à la fin du mois de juin 2020.

Les assurés entrant dans l'expérimentation devaient :

- ◆ avoir 18 ans et plus ou être rattaché à un ouvrant droit éligible ;
- ◆ avoir une carte Vitale valide ;
- ◆ avoir un compte assuré ouvert et une adresse mail avec autorisation d'utilisation ;
- ◆ avoir consommé des soins (une FSE et plus) dans les 24 derniers mois chez un médecin généraliste et/ou un auxiliaire médical.

Par ailleurs, entre le mois de mars 2020 et la fin de l'année 2021, les agents des CPAM concernées, à l'instar des agents des autres CPAM, ont été particulièrement mobilisés dans la gestion de la pandémie et le suivi des cas covid. Leur capacité à animer l'expérimentation a ainsi été fortement réduite. Enfin, à partir d'avril 2022, la fin de la prestation payée par le GIE pour porter techniquement l'expérimentation a entraîné l'impossibilité d'inscrire de nouveaux assurés dans l'expérimentation.

Le nombre limité de professionnels de santé participant à l'expérimentation est à rechercher dans les nombreux prérequis. Il fallait en effet que les professionnels en question aient été sélectionnés par les éditeurs de logiciels et équipés par ces derniers d'une version adéquate de logiciels de facturation compatibles, développés à leurs frais par les éditeurs, sans aide financière des pouvoirs publics, sans que ne soit pour autant garantie la pérennité de l'expérimentation. Ces professionnels de santé identifiés ont fait ensuite l'objet d'une sélection par l'Assurance maladie. Il leur a également été demandé un consentement explicite sous la forme d'un écrit à faire parvenir à l'Assurance maladie.

Les choix faits ont conduit à une première expérimentation réduite sur le plan quantitatif. Néanmoins, les animateurs du projet d'application carte Vitale considèrent que **les enquêtes qualitatives réalisées auprès des utilisateurs a posteriori, largement positives**, se sont révélées utiles dans la conduite subséquente des travaux.

D'après le GIE SESAM Vitale, les professionnels de santé expérimentateurs ont souligné l'aspect novateur de l'application carte Vitale, le bénéfice pour le patient d'avoir ses droits toujours à jour, l'utilisation sans contact répondant aux contraintes sanitaires, le fait de ne plus rencontrer de bugs liés à la carte Vitale physique lorsqu'elle n'est pas reconnue par exemple et l'appui par les Conseillers Informatique Service (CIS) de l'Assurance Maladie lors de l'installation et à l'utilisation.

Les premiers retours des assurés expérimentateurs montrent qu'ils sont à 70% très satisfaits et 26 % assez satisfaits du premier processus d'activation de l'application carte Vitale¹⁶ qui, pour rappel n'était pas un enrôlement biométrique. Ce taux de satisfaction global de 96 % est rassurant sous réserve que le recueil des avis n'ait pas été biaisé par une réponse à un questionnaire en présence de l'expérimentateur et en prenant en compte que le public interrogé était motivé pour participer à l'expérimentation et sélectionné sur plusieurs critères (cf. *supra*).

En parallèle, des cahiers des charges ont été diffusés en octobre 2020 pour faire évoluer les logiciels des professionnels de santé et les rendre compatibles à l'usage de l'application carte Vitale en facturation¹⁷ et pour les téléservices de l'Assurance Maladie.

À la fin du mois d'août 2022, 82 logiciels avaient été agréés ce qui représente un potentiel de déploiement de ces éditeurs de 43,4 % des professionnels de santé libéraux (76,8 % pour les pharmaciens, 64,7 % pour médecins et 53,6 % pour dentistes).

Au 15 novembre 2022, il y avait 50 105 professionnels – sur près de 536 000 au total (cf. annexe I) - effectivement équipés d'une version de leur logiciel compatible avec l'usage de l'ApCV. Il semblerait donc qu'une partie importante des professionnels n'aient pas, à l'automne 2022, actualisé leurs solutions informatiques dont les mises à jour sont parfois payantes.

2.2.2. La CNIL approuve le cadre fixé pour la première expérimentation de l'ApCV et, prend notamment acte de l'aspect non obligatoire de l'application carte Vitale et des limitations fixées

Dans l'ensemble la CNIL relève, dans sa première délibération concernant l'expérimentation d'une application carte Vitale¹⁸, peu de points à corriger.

Elle note que **l'application carte Vitale comprendrait dans sa version cible un enrôlement biométrique par reconnaissance faciale, avec intervention humaine, pour attester de l'identité de la personne ayant téléchargé l'application** mais aussi pour permettre à l'e-carte vitale, à la différence de la carte vitale « physique », d'être utilisée par les patients comme **moyen d'identification électronique afin de bénéficier des services et outils numériques** visés à l'article L.1110-4-1 du CSP.

Elle prend bien connaissance des limitations et garanties fournies aux assurés notamment :

- ♦ une durée de conservation des données biométriques de trois mois à compter de l'activation de l'ApCV au terme duquel elles sont détruites.

¹⁶ Source : Expérimentation application carte Vitale, Point de situation mars 2022, GIE SESAM Vitale, CNAM

¹⁷ Cf. *infra* Addendum 8 au § 2.3.6

¹⁸ Délibération n°2021-031 du 18 mars 2021 portant avis sur un projet de décret prorogeant et étendant l'expérimentation d'une « e-carte d'assurance maladie ».

Annexe IV

- ◆ une participation à l'expérimentation sur la base du volontariat avec un traitement de données biométriques propre à cette expérimentation ; les personnes ne souhaitant pas voir leurs données biométriques traitées pourront toujours bénéficier d'une prise en charge au moyen d'une carte vitale « physique ».
 - La Commission comprend que les personnes pourront s'opposer au traitement de leurs données à caractère personnel au moment de l'affichage des CGU de l'application carte Vitale, ce qui entraînera le refus d'entrée dans l'expérimentation.
 - Afin de garantir la transparence du traitement vis-à-vis des personnes, la Commission invite le ministère à préciser les limitations et les modalités d'exercice du droit d'opposition et d'effacement dans le décret.
- ◆ une sécurisation de l'ApCV par un code secret spécifique aux fins de protection des données et pour éviter l'usurpation d'identité en cas de vol du smartphone.

La CNIL prend acte que **l'application carte Vitale vise à devenir un fournisseur d'identité de niveau eIDAS substantiel pour les fournisseurs de service** destinés aux assurés tels que les portails web et les applications mobiles de l'assurance maladie, de la sphère santé-sociale, et ceux utilisant France Connect. A cet égard, la Commission considère que la vérification d'identité en ligne doit reposer sur des mécanismes techniques minimisant et sécurisant les données traitées. Les travaux actuels autour de l'identité numérique doivent permettre d'améliorer les techniques de vérification qui reposent aujourd'hui sur l'analyse de pièces « papier » au profit de mécanismes reposant sur des composants électroniques, des mécanismes cryptographiques et des flux d'échanges sécurisés (CNIe, passeport, ALICEM, France Connect), qualifiés au sens d'eIDAS.

La Commission relève que l'AIPD détaille de manière très complète l'ensemble des aspects techniques liés à l'application et à ses usages, ainsi que les risques et les mesures pour les réduire. Le ministère a également répondu aux demandes de compléments émises par les services de la Commission. Il en ressort que les modifications portées par le projet de décret ont fait l'objet d'une approche de « Privacy by design » très poussée.

Concernant **les risques liés à une indisponibilité de l'ApCV, il a été précisé que celle-ci devra pour l'instant être considérée comme un support complémentaire à la carte vitale physique**, qui continuera à être délivrée et devra être conservée par les assurés ; ceci tient compte également du temps nécessaire pour la mise à jour des logiciels des nombreux professionnels de santé en ville et des établissements de santé. La Commission en prend acte et estime en outre nécessaire, au regard de ces risques mais également des enjeux d'inclusion numérique, de garantir la délivrance d'une carte vitale physique en cas de pérennisation du dispositif.

La nécessité de la biométrie à l'enrôlement sur l'ApCV n'a pas été appréciée par la CNIL, qui a laissé cette question en suspens dans l'attente d'un bilan plus complet. **Pour cet enrôlement, il est à noter que la CNIL renvoie préférentiellement vers le service de garantie de l'identité numérique (SGIN), et une dérivation de l'identité numérique régalienn.**

L'ApCV n'était ni obligatoire, ni systématique et la finalité de l'usage de la biométrie n'étant pas la lutte contre la fraude mais l'identification de l'assuré et la protection de ses données de santé, l'enrôlement biométrique a été estimé compatible sur le plan juridique avec le cadre national et européen par la CNIL.

2.3. Une seconde phase des expérimentations est conduite depuis septembre 2022 et vise au déploiement d'une application cible intégrant un enrôlement biométrique

2.3.1. La seconde expérimentation à la différence de la première intègre une procédure d'enrôlement biométrique

La première mouture de l'expérimentation lancée en 2019 n'intégrait pas de biométrie. Dans la seconde version testée de l'application carte Vitale, un traitement biométrique intervient lors de la vérification d'identité à distance effectuée lors de l'activation de l'ApCV. Cette vérification s'effectue conformément au référentiel « Prestataire de Vérification d'Identité à Distance » établi par l'ANSSI en avril 2021.

Dans ce traitement, l'assuré doit prendre une vidéo de sa pièce d'identité (selfie) et de lui-même ; cette vidéo est ensuite automatiquement analysée pour vérifier la conformité entre la photo de la pièce d'identité et le visage capté en vidéo, tout en s'assurant qu'il s'agit bien d'une personne réelle et d'une pièce d'identité valide. En cas de résultat positif suite aux opérations biométriques par algorithme, l'ensemble est ensuite validé par un opérateur humain.

Une fois cette opération d'enrôlement de l'utilisateur effectuée, l'application carte Vitale est activée. Il n'est pas prévu de traitement biométrique ultérieur, c'est à dire à l'usage chez le professionnel de santé ou en officine. Un code secret à 6 chiffres, choisi par l'utilisateur, permet de déverrouiller l'application carte Vitale.

2.3.2. Si la biométrie à l'usage a été écartée après une étude approfondie par l'Assurance maladie et le GIE, un enrôlement biométrique par reconnaissance faciale a été retenue pour permettre une labellisation eIDAS de niveau substantiel

Un enrôlement biométrique est considéré comme nécessaire dès la naissance du projet, afin de satisfaire des conditions de sécurité suffisantes dans l'association entre l'application, le smartphone et l'assuré porteur de l'application. Dès le début du projet, les équipes engagent donc avec la CNIL des travaux pour déterminer les articulations entre les objectifs de l'application carte Vitale et les contraintes qu'emporte l'intégration d'un traitement biométrique.

Pour améliorer le niveau de sécurité, dans le respect d'une norme e-IDAS de niveau substantiel, l'exigence d'un enrôlement prévu comme automatique et à distance, la prise en compte des technologies matures et de l'acceptabilité différenciée des technologies biométriques par la population et, surtout, l'utilisation comme référentiel de la photographie d'identité ont conduit l'équipe projet à **retenir la reconnaissance faciale comme moyen pour garantir que la personne utilisant le smartphone corresponde à celle identifiée comme assuré dans les bases de l'Assurance maladie.**

La question de la biométrie à l'usage n'intervient que plus tard, en 2021, faisant suite aux débats au Parlement sur la lutte contre la fraude aux prestations de l'Assurance maladie. Une étude sur la biométrie à l'usage a été réalisée par la Caisse nationale d'Assurance maladie avec l'expertise du GIE SESAM Vitale. Elle a été achevée en septembre 2021. Plusieurs prérequis ont été posés en amont pour en fixer le cadre technique, financier et éthique. A ce titre, 3 conditions ont été posées par la direction de la sécurité sociale :

- ◆ aucune centralisation des données biométriques ne doit être effectuée,

Annexe IV

- ◆ le professionnel de santé ne doit pas avoir d'action supplémentaire à réaliser en lien avec la biométrie pour l'utilisation de cette carte ;
- ◆ il ne doit pas être nécessaire que l'assuré se rende physiquement dans un point d'accueil de l'assurance maladie pour effectuer l'enrôlement biométrique.

Plusieurs technologies biométriques ont été étudiées au regard de l'objectif de lutte contre la fraude qui motive l'étude. Cette étude conclut qu'aucune d'entre elles n'est en mesure d'apporter, en même temps, un niveau satisfaisant de fiabilité du contrôle de l'identité et une capacité de déploiement à l'échelle de l'ensemble de la population (cf. Encadré 1).

Les vérifications à distance pour l'enrôlement reposent d'abord sur la pièce d'identité. Le seul élément biométrique présent sur une captation de la pièce d'identité est la photographie qu'elle comporte. C'est donc le point d'entrée du contrôle biométrique permettant d'authentifier le lien entre la personne qui manipule le smartphone et l'identité déclarée à l'enrôlement.

Les règles appliquées à l'enrôlement biométrique se fondent sur le référentiel Prestataires de vérification d'identité à distance (PVID) développé par l'ANSSI qui a une portée pour des solutions d'identité numérique dans le domaine public mais aussi pour des secteurs marchands comme les banques. Avec l'application de ce référentiel, un contrôle humain vient compléter le contrôle algorithmique (cf. Encadré 2).

Encadré 2 : Référentiel PVID et mise en œuvre par le projet ApCV

Le référentiel PVID développé par l'ANSSI repose sur le postulat que le principal axe de sécurité est le fait qu'il n'est pas possible d'avoir une prise de décision basée à 100% sur les algorithmes. Un mode hybride de validation des demandes d'activation est introduit. Un algorithme peut automatiquement rejeter un dossier de manière automatique. En revanche, toute validation doit reposer sur une validation par un humain sur la base de contrôles hybrides. Au flux vidéo imposé pour capter les informations nécessaires à la validation du profil, des mécanismes d'anti-rejeu, permettant de lutter contre des fraudes, sont introduits pour éviter les piratages (« deepfakes »). En effet, les algorithmes d'IA peuvent être leurrés mais l'anti-rejeu, passant par une consigne à appliquer lors de la captation du flux vidéo par l'assuré, rendent l'opération de falsification plus difficile à réaliser (il peut s'agir par exemple d'une obligation de sourire pendant la captation vidéo ou de cligner de l'œil).

Avec le référentiel PVID, il revient donc à l'ANSSI de qualifier les acteurs prestataires, laissant donc au GIE l'exercice d'un choix rendu plus aisé sur le plan technique puisque celui-ci n'a pas à porter la charge de vérification de la performance de ces intervenants. A date, les prestataires PVID n'ont pas encore été qualifiés par l'ANSSI qui conduit leur passage en revue.

Par le biais de prestataires PVID, le projet ApCV achète un service qualifié PVID qui est déterminé en fonction du cahier des charges du projet. Cette méthode a semblé également la plus adéquate pour assurer une vérification technique de la biométrie à distance, dans le but d'éviter un processus d'enrôlement lourd supposant un face-à-face dans les caisses primaires d'assurance maladie.

Source : Mission d'après ANSSI et GIE SESAM Vitale.

La fraude à l'enrôlement est rendue difficile par la présence de plusieurs axes de défense. Notamment, le fraudeur devrait fournir, en plus de fausses pièces et d'un piratage par *deepfake* de la vidéo selfie en mouvement, une adresse postale similaire à celle de l'assuré légitime, une adresse courriel similaire avec, pour cette dernière, la capacité à s'y connecter.

2.3.3. La 2^e expérimentation fait également l'objet d'un avis de la CNIL qui rappelle que le recours au SGIN devrait être privilégié pour l'enrôlement sur l'ApCV

Dans sa délibération n° 2022-097 du 8 septembre 2022 portant avis sur un projet de décret relatif aux moyens d'identification électronique interrégimes, la CNIL fournit un nouvel avis sur l'ApCV.

Annexe IV

La CNIL se prononce notamment sur un projet de décret ouvrant la voie à la généralisation de l'expérimentation e-carte Vitale. Elle rappelle qu'elle a eu plusieurs fois l'occasion de fournir un avis à ce sujet, en 2018, en 2020 puis en 2021 (cf. *supra*).

La CNIL rappelle que le traitement biométrique pour l'authentification des personnes lors de leur enrôlement pour la création de leur e-carte Vitale est fait afin de permettre à cette personne d'attester de son identité. Cette fonctionnalité vise à s'assurer que le titulaire de la e-carte Vitale est bien celui qu'il prétend être au moment de l'enrôlement pour la création de cette carte. Il est remarqué qu'elle n'a pas pour but de vérifier l'identité de la personne à chaque usage.

La Commission accueille très favorablement le fait de laisser à l'utilisateur le choix entre l'utilisation d'une carte Vitale physique, accessible à tous, et d'une e-carte Vitale. Elle considère que le caractère facultatif et volontaire de l'obtention d'une e-carte Vitale n'est pas de nature à remettre en cause la base légale du traitement.

La Commission estime aussi que le développement d'une e-carte Vitale, proposée au public de façon facultative sous forme d'application mobile, offre des fonctionnalités innovantes et favorise le déploiement du numérique dans le domaine de la santé. Un tel dispositif participe au service public de la santé et de la sécurité sociale et permet de simplifier l'accès à ces services par certains publics

La Commission rappelle l'existence du service de garantie de l'identité numérique (SGIN), un moyen d'identification électronique permettant aux usagers, détenteurs d'une carte nationale d'identité électronique (CNIe), de s'identifier et de s'authentifier auprès d'organismes publics ou privés, en utilisant leur téléphone portable, dès lors qu'il est doté d'un dispositif permettant la lecture sans contact du composant électronique de la CNIe et d'une application mobile spécifique. Le processus d'enrôlement pour la création du moyen d'identification électronique au sein du SGIN s'appuie sur une interaction en présentiel avec un agent public sans analyse biométrique. **La Commission considère que le recours au SGIN devrait être privilégié et l'enrôlement sur l'ApCV par reconnaissance vidéo progressivement abandonné.** Les ministères ont précisé que le parcours d'activation de la e-carte Vitale depuis l'application SGIN ne sera pas opérationnel avant 2023 et qu'il concerne, pour l'instant, un nombre limité de personnes disposant d'une CNIe.

La Commission attire la vigilance des ministères sur les points suivants.

- ◆ les mesures de sécurité mises en œuvre par le fournisseur du socle de sécurité de l'application, qui n'a pas encore été sélectionné, devront être précisées et les risques traités en conséquence ;
- ◆ l'usage de deux facteurs pour l'authentification de proximité du professionnel de santé n'est pas encore confirmé. Une fois la décision sur ce point prise, elle devra être mise à jour, en tenant compte des risques afférents pour les personnes concernées ;
- ◆ la Commission prend acte de ce que l'hébergement du traitement sera confié à un prestataire qualifié SecNumCloud. Les mesures de sécurité mises en œuvre par l'hébergeur devront être précisées dans l'AIPD ;
- ◆ la Commission rappelle que les responsables de traitement devront être attentifs aux transferts de données hors de l'Union européenne et aux possibilités d'accès à des données traitées sur le sol européen qui pourraient être liés à la prestation d'hébergement choisie et au « kit de développement » utilisé pour le socle de sécurité de l'application ;
- ◆ enfin, la fonctionnalité permettant d'activer l'application e-carte Vitale « *par dérivation de l'identité de la carte nationale d'identité électronique* », ainsi que la fonctionnalité de délégation d'une e-carte Vitale, devront être détaillées dans l'AIPD, avec le traitement des risques afférents, préalablement à leur mise en œuvre.

Annexe IV

Dans son avis du 18 mars 2021 sur l'extension de cette expérimentation en termes de périmètre et de durée, la Commission avait réitéré sa demande de disposer d'un bilan détaillé, en particulier sur l'apport de l'utilisation de données biométriques, et son articulation avec d'autres outils permettant de gérer des identités numériques tels que France Connect ou le Service de garantie de l'identité numérique (SGIN).

La CNIL a demandé un bilan complet de la seconde phase de l'expérimentation pour porter une appréciation plus circonstanciée sur la généralisation. Le Gouvernement s'est engagé à fournir à la CNIL un bilan à la mi- 2023 puis en 2024 avant une généralisation effective.

2.3.4. La procédure d'enrôlement, sécurisée par une validation finale humaine, conformément au référentiel PVID de l'ANSSI, comprend un rapprochement biométrique par algorithme pour authentifier le porteur du smartphone

Après validation des conditions générales d'utilisation, l'assuré renseigne son NIR soit :

- ◆ par saisie manuelle du numéro de sécurité sociale ;
- ◆ ou par scan de la carte vitale (ou attestation)

Un contrôle d'éligibilité est fait sur la base du numéro saisi, les conditions d'éligibilité recouvrent notamment de manière non exhaustive le fait d'être assuré à un régime d'assurance maladie obligatoire, le fait d'avoir 16 ans ou plus et, dans un premier temps, le fait de ne pas être sous tutelle ou curatelle et d'habiter dans la zone géographique ouverte à l'expérimentation.

Lors d'une troisième étape, le courriel de l'assuré fait l'objet d'une validation par la saisie sur l'application d'un code à 6 chiffres reçu sur l'adresse courriel renseignée. Le mail est nécessaire pour finaliser l'activation et les usages d'identité numérique à distance avec France Connect.

En quatrième étape, un flux vidéo de selfie du visage est enregistré sur le serveur du PVID sans interruption. Il faut donc une connexion réseau obligatoire pendant toute la durée de cette opération. Ce flux vidéo de l'assuré apporte une preuve du vivant par la détection de micro-mouvements. L'assuré doit également envoyer un scan de sa pièce d'identité (carte nationale d'identité, passeport ou titre de séjour) recto et verso.

Le dossier est ensuite en attente de validation. Un contrôle d'identité (contrôles des traits extraits de la pièce avec les référentiels MRZ, et contrôle croisé entre ces traits et ceux renseignés dans les bases de l'Assurance maladie) et un contrôle de validité du titre (n'utilisant pas DOCVERIF mais s'intéressant à la période de validité du titre) sont opérés. Cette étape peut durer jusqu'à 48 heures.

Les contrôles sont délégués au prestataire Tessi, prestataire de vérification d'identité dont les agents procèdent aux vérifications d'authenticité de la pièce d'identité, de validité du titre, aux vérifications sur la base du selfie vidéo que l'utilisateur est vivant et réel afin d'éviter les « deepfakes » ou les photos truquées.

L'ajout d'un contrôle humain systématique exigé par l'ANSSI est ainsi une condition de sécurité respectée. Le protocole suivi doit amener à contrôler le format du titre, les éléments de sécurité du titre, la photo, les données du document lisibles, la cohérence des pièces fournies, la preuve du vivant par vision de la vidéo systématique, le contrôle biométrique.

Annexe IV

Le contrôle biométrique permet de procéder à un rapprochement algorithmique entre les traits du visage CNI et ceux extraits de la vidéo selfie. Sur cette base, la vérification par un humain permet d'intervenir. L'analyse biométrique fournie par IA peut fournir une confirmation ou un rejet franc ou, en troisième cas, un résultat incertain. Ces trois états de réponse sont déterminés par une méthode de scoring et de positionnement de seuil déterminant les scores. La qualité de ce rapprochement algorithmique des éléments biométriques repose sur le savoir-faire des industriels, c'est-à-dire des prestataires PVID *in fine* qualifiés par l'ANSSI.

La finalisation du parcours usager s'opère avec l'acquisition des données de l'utilisateur sur le smartphone (services Inter régime), soit l'identité AMO ouvrant les droits et renseignant les bénéficiaires (ayants droit, les données de l'état civil issues de la pièce d'identité (uniquement pour l'utilisateur), l'INS de l'utilisateur récupéré lors de la vérification de l'identité, l'email et la photo qui est conservée dans l'application.

2.3.5. La présérie initialement testée à partir de septembre 2022 a montré d'importants dysfonctionnements dans la procédure d'enrôlement des assurés

En septembre 2022, le programme application carte Vitale a franchi une nouvelle étape avec le lancement d'une présérie pour tester une version améliorée de l'application sur un nombre limité d'assurés (quelques dizaines) dans les départements de la première expérimentation (Rhône et Alpes-Maritimes) et de la Sarthe.

Cette présérie ne s'est pas avérée immédiatement opérationnelle pour une diffusion à un plus large public. Elle a montré la nécessité d'améliorer les performances de la phase d'activation initiale de l'application carte Vitale. A la date de la mission, des corrections étaient en cours pour améliorer l'expérience utilisateur en vue d'une ouverture à un plus large public au printemps 2023.

La présérie application carte Vitale a été lancée dès fin août, auprès des agents du GIE SESAM-Vitale. Puis, à partir du 6 septembre, elle a été étendue auprès des agents des CPAM des trois premiers départements : le Rhône (69) et les Alpes Maritimes (06), départements de l'expérimentation, et la Sarthe (72).

À partir du 12 septembre, une nouvelle extension a eu lieu auprès des agents des CPAM de 5 autres départements : la Loire-Atlantique (44), le Puy de Dôme (63), le Bas Rhin (67), la Saône et Loire (71), et les caisses du département de Seine Maritime (76). Au 5 octobre, la MGEN a intégré la présérie et lancé l'inscription de ses agents. Une vingtaine de volontaires ont été répertoriés.

La première partie des tests de la présérie concerne les tests sur l'activation de l'application carte Vitale. La seconde partie des tests, qui a débuté une semaine après la première, concerne les tests d'usage en facturation auprès de professionnels de santé volontaires.

La présérie (activation et usage) avec les agents caisses ne concerne que la version Android. La version iOS n'a été testée que pour l'activation avec 34 agents du GIE SESAM-Vitale, sur une V0 iOS

Au 3 octobre 2022, on comptait 1 230 agents volontaires pour participer à la présérie sur les 8 départements identifiés. La version iOS de la présérie n'étant pas finalisée, le téléchargement de l'application n'a pu être fait que par les smartphones fonctionnant sur Android.

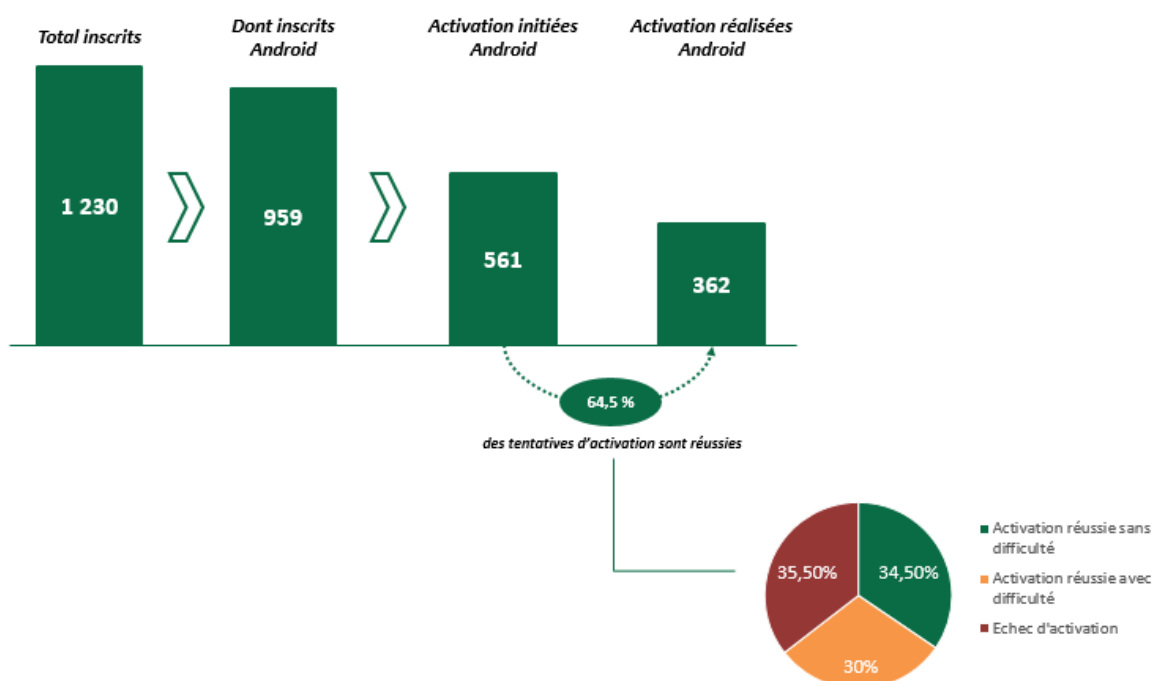
Sur les **959 inscrits** Android, 828 ont reçu le lien de téléchargement. 561 activations ont été initiées sur Android et, *in fine*, **362 activations ont été réalisées, soit 64,5 %** (cf. Graphique 5).

Annexe IV

Les inscrits étaient les agents s'étant fait connaître de leur service et ayant marqué dans un premier temps un intérêt. Inscrits sur une liste blanche, ils étaient autorisés à accéder au store et à télécharger l'application. Tous n'ont donc pas transformé cet intérêt jusqu'à la réalisation d'un parcours d'activation.

En revanche, le taux de transformation d'une activation initiée en activation réussie interroge. Si au 3 octobre, 64,5% des tentatives d'activation sont réussies, **seules 34,5% des activations sont réussies sans rencontrer d'erreur** lors de l'étape du flux vidéo. **L'échec à l'activation s'élève au demeurant à 35,5 % des activations initiées.**

Graphique 5 : Nombre d'inscriptions, d'activations initiées et d'activations réussies dans le cadre de la présérie de septembre 2022



Source : Mission d'après CNAM « Synthèse sur la présérie application carte Vitale de Juillet à Décembre 2022 ».

Les parcours d'enrôlement sont impactés par une instabilité des flux vidéo. Notamment des pertes de connexion ont constitué le problème central. Ces difficultés entraînent une dégradation forte de l'expérience utilisateur pour les assurés.

Les deux tiers des échecs à l'activation sont en effet dus à des difficultés à réaliser le flux vidéo :

- ◆ la vidéo n'est réalisée avec succès dès le premier essai que dans 33 % des cas ;
- ◆ 60 % des utilisateurs rencontrent une difficulté au moment de la vidéo de leur pièce d'identité selon les retours de l'enquête ;
- ◆ 40 % des utilisateurs rencontrent une difficulté au moment de la vidéo de leur visage, qui a pour but de valider la preuve du vivant, et de valider la reconnaissance entre le visage et la pièce d'identité.

Un paramétrage élevé en termes de sécurité, avec une sensibilité trop importante à la bande passante, et des micro-coupures de réseau entraînent trop souvent un échec de l'enrôlement. Dans le cas de la CPAM 69, il a été ainsi constaté que seuls 30 % des agents de la caisse sont parvenus à s'enrôler sans bug.

La CNAM notait ainsi qu'au mois de septembre, il fallait 4 tentatives de l'utilisateur pour réussir à s'enrôler lors de l'étape vidéo contre 1,8 tentative en décembre 2022.

Annexe IV

Dans une moindre mesure, il a été constaté des problèmes de rapprochement d'identité et de reconnaissance des assurés dans les bases de l'assurance maladie obligatoire ainsi que des rejets sur les photos retenues pour inscription dans l'application (des problèmes relatifs aux règles de rapprochement de l'identité). Dans ce dernier cas, certains rejets ont été réalisés, en revanche, pour des causes légitimes comme par exemple des photos non recevables ou des pièces d'identité périmées.

Du côté des professionnels de santé, le système ApCV pour la facturation était opérationnel, en dépit de plusieurs anomalies constatées (cf. *infra*). Parmi les difficultés rencontrées, on peut mentionner les suivantes :

- ◆ le QR code n'est pas lisible lorsque le téléphone est utilisé en mode sombre ;
- ◆ des échecs d'authentification ont été constatés notamment faute d'autorisations ouvertes par les logiciels ;
- ◆ des cas de résumés de dépenses de soins n'ont pas été reçus.

Sur la base de ces résultats, des travaux correctifs ont été engagés (cf. Encadré 3). En particulier, afin de résoudre l'importante difficulté constatée dans la phase d'enrôlement des assurés, les travaux se poursuivaient en 2023 sur la correction du paramétrage du SI central, sur la résorption des microcoupures et sur les consignes fournies aux personnes validant le processus. L'essentiel du problème se concentrant sur les sujets de réseaux, l'amélioration de la bande passante apparaît comme la piste principale d'amélioration à court terme de l'expérience usager.

La correction à apporter est cruciale car, comme le notent la CNAM et le GIE SESAM Vitale dans la synthèse faite sur les résultats de la présérie en date du 7 décembre 2022, « *le taux d'activation réussies de 64.5 % est caractérisé par un nombre de tentatives importantes et au-delà de ce qu'un assuré lambda ferait* ».

Encadré 3 : Principales corrections prises à la suite de la présérie de septembre 2022

Adaptation des CGU (nouveau décret) et ajout d'une mention sur l'accessibilité de l'application.

Activation de l'application :

- Mise en place d'un test préalable sur connectivité minimale nécessaire ;
- Amélioration des performances lors de la capture du titre d'identité et prise du selfie (diminution bande passante minimale nécessaire) ;
- Amélioration des consignes à l'utilisateur ;
- Correction problème de scan du NIR sur modèles HUAWEI P30 et autres ;
- Meilleure reconnaissance du NIR de l'utilisateur dans les référentiels assurés des régimes ;
- Prise en compte des villes de naissance avec arrondissement ;
- Renforcement des consignes auprès des opérateurs pour valider la photo finale inscrite dans l'application.

Usage chez un Professionnel de Santé :

- Amélioration du tutoriel pour prendre en compte l'absence de NFC sur le téléphone ;
- Forçage en mode white mode lors de l'affichage d'un QR Code ;

Correction de bugs divers.

Source : GIE SESAM-Vitale.

Le volume constaté, en nombre de FSE, en nombre d'assurés enrôlés et de professionnels de santé équipés est très faible.

Annexe IV

Dans cette présérie, en particulier, il est à noter qu'il n'y a pas eu d'expérimentation de l'application par un professionnel de santé seul avec un assuré social. **Toutes les factures ont été réalisées par des CIS des 8 départements concernés avec des professionnels de santé équipés, sur rendez-vous.** Ces tests d'usage ont donc été réalisés sous observation voire avec l'aide d'un agent de la caisse primaire spécialisé en informatique. Les factures ont fait l'objet d'une sécurisation SESAM-Vitale afin de tester la chaîne de liaison SI néanmoins.

Seules 51 feuilles de soins électroniques ont été réalisées en 44 rendez-vous entre le 19 septembre et le 21 octobre 2022. Dans 26 cas, la réalisation s'est déroulée correctement. Dans 49 % des cas, une anomalie a été détectée (cf. Encadré 4). D'après la DDGOS de la CNAM, il n'a pas s'agit là d'anomalies empêchant la facturation, plusieurs étant liées au fait que ces facturations se faisaient à 0 euros. Les feuilles de soins ont pu être établies et le flux de transmission a été constaté en bout de chaîne informatique. Quant aux autres anomalies, elles ont fait l'objet de rapides travaux de correction à la fin de l'année 2022 et au début de l'année 2023.

Encadré 4 : Bilan des anomalies remontées lors des tests d'usage de la présérie auprès des professionnels de santé

Problématiques liées au SI :

- Problématique pour lire les applications carte Vitale réelles/démos au format base45 en production.
- Problématique pour lire le QR Code quand le dark mode est activé sur le smartphone (évolution sera mise à dispo avec la nouvelle version).
- Non réception de l'information de la dépense de soin dans l'onglet "activités".
- Les données de l'application carte Vitale ne sont pas correctes □ Erreur - ApCV_601 - OTP invalide.
- Impossible d'interpréter le retour de l'ApCV authentification quand il n'y a pas de bénéficiaire.

Problématiques autres :

- L'ergonomie du logiciel du professionnel de santé (LPS) pourrait être un frein à l'adoption de l'ApCV par les professionnels de santé. Il convient à minima de prévoir une Fiche d'Information pour inviter les éditeurs à améliorer l'ergonomie de leur LPS dans la facturation avec une application carte Vitale.
- Plusieurs éditeurs rencontrent des difficultés pour lire le contenu de l'application carte Vitale lorsqu'il est en base45. L'application carte Vitale de test éditeur étant au format base64.
- Impossibilité d'interpréter le retour de l'application carte Vitale quand il n'y a pas de bénéficiaire.
- Alimenter une FAQ avec les causes possibles de l'OTP invalide (2 cas non expliqués).
- Anomalie d'alimentation de la table des LPS autorisés (côté CNDA).

Source : CNAM Bilan de la présérie.

Enfin, la mission ne peut se prononcer sur la capacité de cette application cible lancée depuis fin août 2022 en présérie à tenir une charge sensiblement plus élevée que celle enregistrée par le téléservice ADRI à l'heure actuelle (25 % des flux de FSE).

D'une part, aucune opération spécifique de test de charge n'avait été conduite sur la technologie destinée à être déployée à un plus large public avant janvier 2023. Il est apparu au début de l'année 2023 que la version cible testée en présérie ne pouvait supporter trois connexions simultanées, conduisant à réviser l'architecture du produit en février 2023. Les tests de charge effectués depuis se sont avérés plus concluants.

D'autre part, comme indiqué supra, le taux de disponibilité du téléservice ADRI est fonction des capacités de charge de son infrastructure. L'appel de ce téléservice, depuis l'application carte Vitale, pourrait donc être bloqué au niveau de l'infrastructure de l'Assurance maladie (« DESIR ») qui agit comme un fusible (régulation du nombre d'appels)¹⁹.

2.3.6. Si une présérie a été déployée au mois de septembre 2022, l'ouverture de la première version cible de l'application au public des huit premiers départements concernés a été décalée de l'automne 2022 au mois de mars 2023

À compter de septembre 2022, une présérie de la version cible de l'application carte Vitale a donc été testée auprès des agents du GIE SESAM-Vitale et de 8 CPAM. Il avait été souhaité, si l'expérimentation s'avérait concluante, une ouverture au grand public de ces départements dès le mois d'octobre. Néanmoins, les résultats de cette présérie démontrant le besoin de corriger plusieurs difficultés constatées ont amené à repousser *a minima* au printemps 2023 l'ouverture prévue au public.

À partir du printemps 2023, il est envisagé une ouverture progressive au public car il faut, en parallèle des enrôlements d'assurés, disposer de professionnels de santé équipés sur le plan SI de logiciels compatibles avec l'utilisation de l'ApCV et, sur le plan matériel, de moyens techniques de lire le QR code ou le signal NFC. Un support utilisateurs sera par ailleurs prévu au niveau des CPAM, à l'accueil ainsi qu'un support téléphonique, pour répondre aux questions qu'assurés et professionnels pourraient avoir lors du déploiement progressif de cette application.

Les constatations effectuées en février 2023 sur les résultats de la présérie ont conduit à prévoir une généralisation progressive sur les 8 départements expérimentateurs *a priori* à compter du printemps 2023, sous réserve d'une finalisation rapide des travaux correctifs entrepris.

L'ouverture à terme prévue ne se ferait pas d'un seul tenant. Un système de jauges serait mis en place sur les stores de téléchargement pour limiter la diffusion de l'application à quelques milliers d'assurés par département afin d'observer auprès de cette population cible le comportement de l'application et les réactions des usagers. L'ouverture plus large n'interviendra que dans un second temps.

Dans le cadre de cette présérie, certaines fonctionnalités n'ont en outre pas été incluses telles que la délégation à un tiers ou l'identification numérique à distance. Le fonctionnement de l'application s'est concentré sur la fonctionnalité classique de la carte Vitale et la sécurisation des flux de facturation.

S'agissant de l'équipement en logiciel compatible avec l'ApCV, essentiel pour un déploiement fluide de cette nouvelle solution, l'Addendum 8²⁰ fixe un objectif de 40 % de pharmaciens équipés et de 20 % des médecins-généralistes équipés en vue de la généralisation. **Au 15 janvier 2023, toutes catégories confondues, le taux de professionnels de santé équipés d'un logiciel compatible avec l'ApCV était de 18,7 %** (cf. Tableau 3).

¹⁹ Le professionnel de santé peut renouveler son appel plusieurs fois avant d'être connecté avec Adri. Aucun message ne lui permet de comprendre le motif de rejet de son appel (point d'amélioration envisagé). Source : CNAM-DDGOS.

²⁰ Un an après le lancement de l'expérimentation application carte Vitale, le GIE SESAM-Vitale a diffusé en octobre 2020 auprès des éditeurs de logiciel l'Addendum 8 au cahier des charges SESAM-Vitale et le Référentiel Dispositif Intégré 4.0 afin qu'ils rendent compatibles leurs solutions. Simultanément, les guides TLSi ont été publiés pour que les industriels puissent également rendre leurs téléservices AMO compatibles avec l'application carte Vitale et garantir ainsi la cohérence du poste du professionnel de santé.

Annexe IV

Tableau 3 : Taux de professionnels de santé équipés d'un logiciel compatible ApCV pour la France entière au 15 janvier 2023 (en %)

-	Toutes catégories	Médecins	Pharmaciens	Autres catégories
France entière	18,7	26,6	67,3	11,4
Dont Alpes-Maritimes	17,7	32,1	61,9	8,11
Dont Rhône	16,9	24,9	64,2	9,61
Dont Sarthe	19,4	23,1	61,9	11,2

Source : GIE SESAME-Vitale.

Des incitations financières ont été et seront prévues au travers de différents instruments pour accompagner le développement des nouveaux logiciels par les éditeurs et l'achat de matériel par les professionnels de santé.

L'avenant 9 de la convention médicale signé à l'été 2021 prévoit des incitations financières à l'équipement (addendum 8) dans le socle du forfait structure et à l'usage de l'application carte Vitale de 280 euros²¹, permettant de couvrir le coût des lecteurs de QR code et NFC dont les prix sont compris entre 150 € et 400 € selon les modèles. La convention pharmaciens signée en 2022 prévoit un indicateur socle « *disposer d'un logiciel référencé Ségur* » donc qui intègre l'Addendum 8 et également une aide de 50€ pour l'usage de l'application carte Vitale.

Dans les négociations conventionnelles avec les médecins de début 2023, la rédaction de la convention était la suivante : « *Cet indicateur valorise l'usage de l'application carte Vitale. Pour valider l'indicateur, le médecin doit transmettre au moins une FSE avec usage de l'application carte vitale. Cet indicateur calculé automatiquement par l'assurance maladie est valorisé à hauteur de 40 points* ». Cette rédaction serait reprise dans le règlement arbitral en cours, confortant le déclenchement de l'incitation financière dès la première émission d'une FSE signée par l'application carte Vitale.

Enfin, avec le programme « Ségur du numérique en santé », l'État finance directement les éditeurs pour qu'ils modernisent les logiciels métiers des médecins, selon un cahier des charges garantissant l'interopérabilité des systèmes d'information, la sécurité des données et l'ergonomie de l'outil au quotidien. Les médecins peuvent ainsi bénéficier d'une prise en charge intégrale par l'État de cette mise à jour²².

2.4. Si les usagers – assurés comme professionnels de santé – sont demandeurs d'une solution dématérialisée, il n'est pas possible au vu de la faible volumétrie des 2 phases de l'expérimentation de conclure positivement à son fonctionnement opérationnel à grande échelle

Les avis des usagers et des professionnels recueillis dans le cadre de la première expérimentation puis de la présérie, en rappelant tout de même leur faible nombre du fait d'un champ très restreint d'expérimentation et donc leur représentativité limitée, **apparaissent positifs.**

Toutefois, le faible volume de factures, d'assurés enrôlés et de professionnels équipés ne permettent pas de conclure en faveur d'un déploiement rapide et à grande échelle de cette application cible.

²¹ Un forfait de 280 euros, soit 40 points à 7 euros le point.

²² Source : [Tout savoir sur le passage au logiciel métier version « Ségur » et la prise en charge de l'État - ameli.fr](#).

Annexe IV

Les principales anomalies liées au fonctionnement général de l'application ont été détectées grâce aux tests en présérie. Le déploiement de l'application sur un périmètre et un échantillon plus large permettra de disposer de davantage de cas d'usage exploitables sur une panoplie de thématiques non encore identifiées. Pendant quelques mois, des bugs sur de plus petites fonctionnalités sont ainsi à prévoir en particulier pour une application qui aura vocation à être utilisée par une grande diversité de smartphones.

Un degré de prudence dans la diffusion progressive de l'application sur les stores de téléchargement est recommandé.

Si un tel produit, offrant une carte Vitale digitalisée à tous les assurés sociaux, est à l'évidence attendu par les usagers et par les professionnels, un lancement trop rapide d'un outil dysfonctionnel (difficultés d'enrôlement, indisponibilité ADRI, ou de certaines fonctionnalités...), entraînerait un risque réputationnel fort pour l'ApCV.

Il est ainsi utile de rappeler l'expérience de l'application « L'identité numérique La Poste » qui permet de sécuriser son identité numérique pour accéder aux services en ligne via France Connect et La Poste avec un identifiant unique. A la date du 27 février 2023, cette application recevait sur le store Android une note de 2,5 sur 5, pour 9 288 avis. Un très grand nombre d'internautes se plaignaient des difficultés rencontrées dans le fonctionnement de l'application et des nombreuses avaries techniques et incidents constatés, attestant de la mise en ligne de versions successives défectueuses entraînant un effet réputationnel négatif. Cette méthode fait courir un risque de rythme d'adoption plus lent de l'application dans l'éventualité où ces premiers testeurs du produit, « *early adopters* », ne téléchargent pas les nouvelles versions corrigées des défauts initialement constatés, voire aillent jusqu'à faire une publicité négative de l'application auprès de leur entourage.

3. La décision de généraliser l'application carte Vitale a déjà été prise avec, néanmoins, un calendrier de mise en œuvre connaissant un décalage du fait des difficultés opérationnelles rencontrées

3.1. Sans attendre les résultats des expérimentations conduites, la décision d'une généralisation a été prise et des travaux en ce sens ont été lancés

Dans le prolongement de l'ordonnance du 12 mai 2021 relative à l'identification électronique des utilisateurs de services numériques en santé, un décret déterminant de décembre 2022 ouvre la voie à la généralisation de l'application carte Vitale.

Le décret en Conseil d'État n° 2022-1719 du 28 décembre 2022 relatif aux moyens d'identification électronique interrégimes, en effet, permet la généralisation de l'application carte Vitale et l'extension des services proposés.

L'application carte Vitale pourra être utilisée à terme comme fournisseur d'identité numérique à distance pour se connecter à des portails web ou applis du monde de la santé social (comme France Connect), ainsi que pour une prise en charge à distance avec les professionnels de santé et établissements de santé (télésanté, préadmission en établissement).

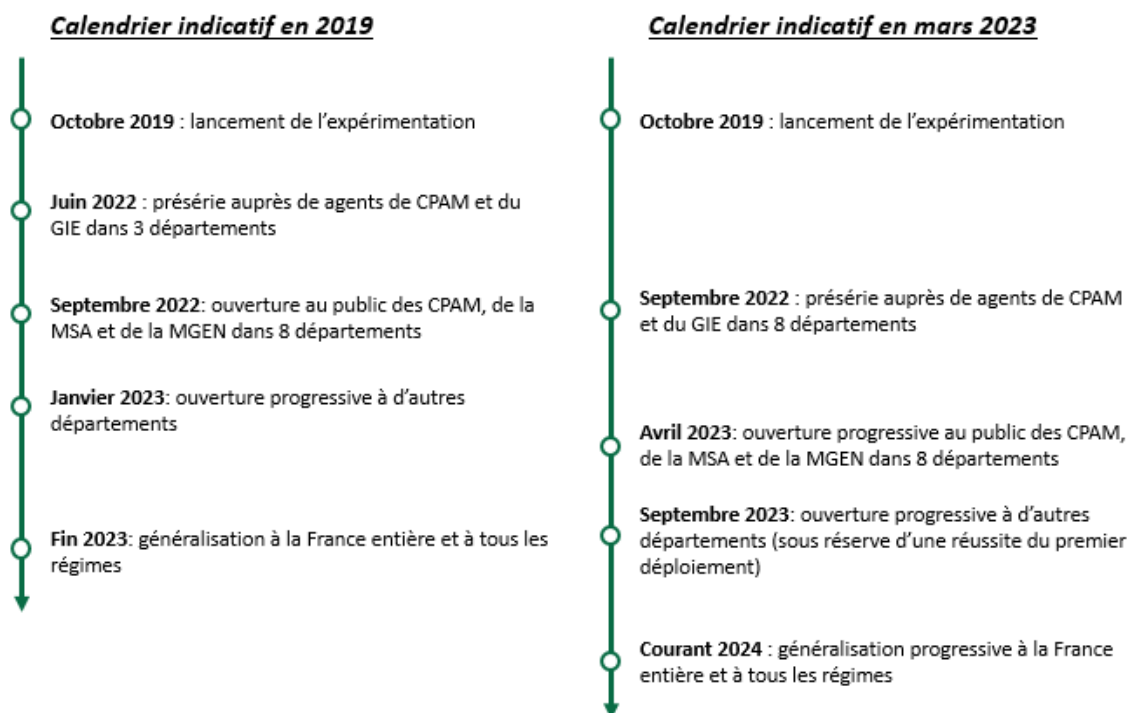
3.2. Le calendrier de déploiement a tendance à s'allonger mais demeure ambitieux

Le calendrier a néanmoins connu d'importants décalages. La présérie, en test entre septembre 2022 et février 2023, devait par exemple être initialement testée en 2021 puis a été décalée à juin 2022 avant de se tenir finalement en septembre 2022.

Annexe IV

Le lancement à destination des assurés des huit départements identifiés devait avoir initialement lieu à la fin de l'automne 2022. Il a plutôt été fait le choix, le 13 septembre 2022, au vu des premiers résultats de la présérie auprès des agents des CPAM concernées et du GIE SESAM-Vitale de décaler cette ouverture. Dans le nouveau calendrier (cf. Graphique 6), l'ouverture plus large, département par département, ou région par région, au public pourrait débuter en septembre 2023 avant une ouverture à tout le territoire en 2024.

Graphique 6 : Calendriers indicatifs à deux moments du projet ApCV en 2019 et en 2022



Source : Mission d'après CNAM et GIE SESAM-Vitale.

Par ailleurs la généralisation de l'application carte Vitale, présentant toutes ses fonctionnalités, repose aussi sur la capacité de l'équipe projet à ouvrir le service Fournisseur d'identité. Il était encore prévu en 2022 une ouverture de ce service en septembre 2023, avec comme premiers usages l'accès à France Connect, le développement d'un pilote pour la préadmission en établissement de santé et l'accès à des services de télésanté. A la mi-février 2023, en revanche, le GIE SESAM-Vitale ne pouvait confirmer à la mission la capacité de l'application à être développée suffisamment vite pour proposer dans les temps impartis ces services.

En parallèle des travaux sont engagés pour permettre aussi tôt que possible, et avec un objectif à l'automne 2023, la dérivation d'identité numérique depuis le SGIN.

Le parcours d'activation par dérivation de la CNIE doit être de courte durée et facilitant par rapport au parcours dit classique en minimisant le nombre d'actions utilisateur. Le parcours d'activation dérivation CNIE doit être de même niveau de sécurité que le parcours dit classique. Le parcours d'activation dérivation CNIE ne doit pas nécessiter de passer par le PVID.

Des critères d'éligibilité déterminent les assurés pouvant utiliser cette voie d'activation. L'utilisateur doit avoir une CNIE française. Il doit être une personne majeure dont l'identité numérique doit être activée, et il doit être en possession du code PIN d'authentification. L'application AppFI doit être installée sur le téléphone de l'utilisateur (qui doit donc être compatible avec l'application).

Annexe IV

Au premier trimestre 2023, une première maquette a été réalisée sur les parcours d'activation de l'ApCV par dérivation de l'identité numérique régaliennne. La CNAM souhaiterait pouvoir réaliser un POC technique – avec une version bêta prête au début de l'année 2024 – et pour objectif de définir une solution technique d'échange entre les applications et de tester en conditions réelles les résultats des échanges entre les systèmes d'information.

Il faut néanmoins récupérer la photo de l'utilisateur. Les travaux sont conduits avec l'ANTS. Il restera la captation photo de la carte Vitale. Le calendrier est fixé dans le décret, à fin 2024 pour un système qui fonctionne. La CNIL considère que cette voie est à privilégier à un enrôlement ad hoc (impliquant donc des prestataires PVID) tel qu'il est organisé actuellement.

3.3. Plusieurs sujets de fond appellent des réflexions complémentaires

3.3.1. Le système cible privilégié, à partir du moment où l'application carte Vitale sera largement adoptée par les assurés, reste à déterminer

Les entretiens conduits par la mission montrent la vision positive portée par l'écosystème du système de santé français sur le développement de l'ApCV et sa diffusion. Les objectifs poursuivis par l'application carte Vitale rejoignent la demande des usagers, des professionnels de santé et de leur représentations et fédérations. Une fédération a en revanche indiqué son inquiétude que d'autres projets, tels que par exemple la mise en place d'une carte Vitale biométrique, vienne retarder le déploiement de l'application carte Vitale.

S'il est souhaité une généralisation rapide de l'application, les interlocuteurs de la mission rappellent également les limites d'une telle solution, en particulier la nécessité de disposer d'un support matériel, en coexistence avec l'application, de portage des droits afin que la fracture numérique n'empêche pas le plein exercice des droits sociaux. Le CNOP rappelle toutefois que la coexistence entre une carte physique et une application carte Vitale représente la solution la plus coûteuse pour l'Assurance maladie²³.

Toutefois, ce soutien à une solution double à moyen terme n'obère pas le besoin de s'interroger sur le système cible visé à terme par les autorités compétentes, dans une articulation entre support physique et support numérique. Or, à la date de la mission, aucune réflexion structurée n'a été conduite ou lancée soit par la CNAM, en interne, soit en association avec les acteurs de la sphère de la santé. L'attention des autorités, des caisses d'assurance maladie et des professionnels, de l'avis de plusieurs interlocuteurs de la mission, est momentanément absorbée par la conduite – et la réussite - du projet d'application carte Vitale.

3.3.2. Quand bien même l'ApCV connaîtrait un succès dans son déploiement à terme, le recours via l'application à la biométrie à l'usage n'apportera que de faibles garanties tout en présentant une probable impraticabilité technique

À moyen terme, le fonctionnement à grande échelle d'une application qui prévoit un enrôlement biométrique conduira à réinterroger le développement via cet outil d'une biométrie à l'usage, c'est-à-dire d'un traitement biométrique valide préalable à l'émission d'un QR code ou validant le fonctionnement d'un lien NFC lors de l'accès aux soins.

²³ Contribution écrite du Conseil National de l'Ordre des Pharmaciens à la mission « carte Vitale biométrique », datée du 13 mars 2023.

Annexe IV

Un tel projet aurait une cohérence avec la mise en place d'un support physique biométrique (carte Vitale biométrique) à l'usage si le choix de cette dernière option était opéré. Dans ce cas, le bilan avantages/inconvénients de l'usage de la biométrie dans le système français de santé publique, tel qu'établi par la mission en annexe V, vaudrait tout autant pour le recours à la biométrie à l'usage dans le cadre de l'application carte Vitale.

Le choix d'une biométrie à l'usage sur l'ApCV, sans pour autant disposer en parallèle d'une carte physique biométrique, présenterait en revanche un intérêt faible car elle n'apporterait aucune garantie d'intégrité sur le principe et s'avèrerait très difficilement praticable sur le plan technique.

Sur le plan de la finalité de ce traitement biométrique à l'usage, si le but est d'améliorer l'ergonomie de l'application, ou de compléter ses fonctions, sans finalité justifiée ou rendue nécessaire, l'impact sur la performance de l'ApCV d'un traitement biométrique à l'usage devrait conduire à écarter cette voie.

Si, en revanche, la finalité est de lutter contre l'usurpation d'identité, l'objection à la mise en place de ce traitement est double :

- ◆ d'une part, il est probable que les fraudeurs ciblés par cette mesure se déportent aisément vers des méthodes d'attestation de leur droit non biométrique, en particulier par l'utilisation d'attestation papier, rendant ainsi la solution biométrique sur l'application inefficace ;
- ◆ d'autre part, la réutilisation des systèmes biométriques embarqués dans les smartphones est inopérante. En effet, il ne serait pas possible de s'assurer de l'intégrité du gabarit retenu dans les solutions biométriques des systèmes d'exploitation des smartphones pour cette biométrie à l'usage. Par conséquent, l'Assurance maladie ne pourrait garantir que l'utilisation courante de l'application carte Vitale soit faite par le titulaire légitime du NIR déclaré (cf. Encadré 5).

D'une manière générale, la biométrie à l'usage sur l'ApCV n'offrirait donc aucune garantie supplémentaire à la sécurisation d'un usage du smartphone déjà protégé par un code ou par une ouverture biométrique. Il est également probable qu'un verrouillage plus important du dispositif sur le smartphone manque la cible.

Encadré 5 : L'utilisation de la biométrie des systèmes d'exploitation de smartphone

Les solutions de biométrie proposées par Apple et les différents constructeurs de smartphones Android sont de plus en plus sophistiquées et de plus en plus utilisées par le grand public pour servir d'authentification à des applications ou même à valider des paiements.

L'enrôlement de l'utilisateur est géré par l'OS, via les paramètres du téléphone. Le gabarit de référence alors créé est stocké de manière sécurisée sur un « coffre-fort » numérique au sein du smartphone (Secure Enclave pour iOS, TEE pour Android).

Lorsqu'une application est déverrouillée par biométrie, l'application ne fait que solliciter la solution biométrique du smartphone, qui récupère un gabarit, le compare au gabarit de référence, et renvoie à l'application le résultat de la comparaison.

Ces solutions ont été développées avant tout pour améliorer l'expérience utilisateur en lui évitant l'usage de mots de passe. Elles ne répondent donc pas directement à une problématique de fraude.

En effet :

- ces solutions ne permettent pas la maîtrise du gabarit de référence (un utilisateur du téléphone peut modifier ce gabarit comme bon lui semble quand il le souhaite, notamment après l'enrôlement ApCV) ;
- le système d'exploitation n'impose pas à l'utilisateur l'utilisation de la biométrie (l'utilisateur peut choisir de déverrouiller l'application avec un code pin au lieu de la biométrie, et ainsi frauder).

En revanche, il pourrait être possible d'utiliser les capteurs des smartphones pour obtenir un échantillon biométrique, puis construire les gabarits et les comparer indépendamment du système d'exploitation du smartphone, en tenant compte des limites suivantes :

Annexe IV

- impossibilité d'utiliser les algorithmes de construction de gabarit et de comparaison présents dans les systèmes d'exploitation (nécessité de développer les algorithmes ou de faire appel à une solution externe) ;
- accès limité à certains capteurs (lecteur d'empreinte inaccessible sur iPhone et sur certains appareils Android).

Source : Mission d'après GIE SESAM-Vitale.

Sur un plan technique, le développement de la biométrie à l'usage sur l'ApCV s'avèrerait en outre difficilement praticable.

Le système d'exploitation Apple, étant fermé, une solution de biométrie à l'usage ne pourrait a priori pas fonctionner sur les smartphones de cette marque.

Dans un environnement Android, une solution de biométrie à l'usage devrait fonctionner sur toute la panoplie de matériel utilisant cette OS, avec des capteurs de nature diverse ou bien calibrés différemment, ce qui est une gageure.

Il est alors utile de reprendre le questionnaire lancé en 2021, lorsque le GIE SESAM Vitale pour fournir des éléments de réponse à ses commanditaires, a établi une étude fouillée sur l'usage de la biométrie finalisée.

Cette étude écarte notamment les modalités biométriques mobilisables par les possesseurs d'un smartphone équipés de capteurs biométriques ou photographiques aux motifs suivants :

- ◆ l'usage des empreintes digitales à partir du capteur propriétaire du smartphone: le parc de smartphones en France ne dispose pas pour une part importante de lecteurs d'empreintes. Apple a décidé de ne plus mettre ce type de capteurs dans ses smartphones. Un déploiement à l'échelle nationale n'est donc pas envisageable. De plus, la robustesse du contrôle biométrique repose la comparaison entre une donnée biométrique de référence contrôlée en amont par l'Assurance Maladie et un nouveau gabarit réalisé au moment de la consultation. Or l'Assurance Maladie ne dispose pas de cette donnée de référence ;
- ◆ la reconnaissance faciale seule (sans reconnaissance du "vivant") : ce contrôle est possible par une comparaison avec la photographie d'un titre d'identité mais la fiabilité du traitement biométrique n'est pas suffisamment importante à ce jour pour garantir un bon fonctionnement en usage courant au quotidien. Considérant que les anomalies d'identification ne peuvent pas être directement assimilées à une fraude et pour ne pas priver l'assuré des services rendus par la carte (notamment l'accès aux droits de la personne et l'émission de la feuille de soins électronique qui est une obligation pour le professionnel de santé et simplifie la gestion des documents de remboursement, voire le bénéfice du tiers payant), l'assurance maladie devrait en tout état de cause mettre en place une solution alternative pour que le professionnel puisse connaître les droits et faire la facturation des soins.

De plus, leurs dispositifs biométriques sont « propriétaires », c'est-à-dire à la main des entreprises propriétaires des systèmes d'exploitation, dont les performances sont très variables d'un appareil et d'une version à l'autre : s'appuyer sur ces dispositifs pourrait conduire à devoir développer une nouvelle application carte Vitale et à réécrire autant d'algorithmes de rapprochement qu'il existe des versions de systèmes propriétaires – le tout étant conditionné à l'accord de leurs concepteurs.

3.3.3. L'impact de l'application carte Vitale sur la fraude à l'Assurance maladie devrait être faible

Les caractéristiques de l'application carte Vitale apportent des garanties de sécurité supplémentaires par rapport à la carte Vitale physique pour lutter contre la fraude à l'usage :

Annexe IV

- ◆ son enrôlement biométrique et sécurisé répondant aux exigences de qualification eIDAS substantiel ;
- ◆ son usage possible uniquement après déverrouillage par code secret ;
- ◆ l'authentification du support à chaque usage : il n'est pas possible d'utiliser une application perdue ou volée ;
- ◆ la désactivation de l'application pour des utilisateurs qui ne serait plus assuré ;
- ◆ un recours systématique aux services de droits déployés par l'assurance maladie pour obtenir la situation administrative de l'utilisateur ;
- ◆ la consultation d'un résumé des dépenses de soins, ce qui pourrait conduire à des signalements par les assurés de professionnels de santé fraudeurs.

Dès lors, la carte Vitale physique, si elle reste en circulation sans comporter de mesure de sécurité complémentaire, deviendra le support privilégié par les fraudeurs, avec l'attestation de droits papier, car elles constitueront une voie de contournement. L'application carte Vitale, n'étant pas obligatoire, les assurés pourront toujours utiliser la carte plastique dans une optique de mésusage ou de fraude (prêt, vol, usurpation d'identité).

Plus problématique est toutefois l'existence duale d'une même carte Vitale pendant un certain temps, et potentiellement une décennie ou plus, sur support physique et sur application, en l'absence de stratégie sur un système cible et exclusif, et des garanties de paiements qui y sont associées.

La coexistence de ces plusieurs supports pour faire valoir des droits sociaux et d'obtenir, en cas de tiers payant, une couverture de sa dépense de soins, présente le risque de généraliser les pratiques de prêt potentiellement frauduleuses.

En outre, les indus nés de l'absence de mise à jour de la carte Vitale physique risquent d'augmenter sensiblement, dès lors que l'utilisation du support physique sera plus sporadique, conduisant à plus d'erreurs dans les facturations.

ANNEXE V

Le recours à la technologie biométrique : avantages et inconvénients

SOMMAIRE

1. LES CAS D'UTILISATION DE LA BIOMÉTRIE EN FRANCE	1
1.1. De quoi parle-t-on quand on parle de biométrie ?	1
1.1.1. <i>La notion de biométrie est très largement définie.....</i>	<i>1</i>
1.1.2. <i>Si les techniques de biométrie portent sur un nombre foisonnant de caractéristiques, seul un nombre restreint est mis en œuvre de manière opérationnelle.....</i>	<i>2</i>
1.2. La performance des techniques biométriques est variable, mais aucune technique ne présente de garantie absolue	3
1.2.1. <i>Les techniques biométriques présentent des caractéristiques différentes ...</i>	<i>3</i>
1.2.1. <i>Les principales techniques biométriques sont soit onéreuses, soit peu acceptables, soit sensibles.....</i>	<i>4</i>
1.3. Entre identification et authentification, les déterminants de l'architecture d'un système biométrique sont multiples.....	7
1.3.1. <i>L'authentification permet simplement de vérifier que l'identité d'une personne est bien celle qu'elle prétend, alors que l'identification est plus intrusive en matière de droits individuels.....</i>	<i>7</i>
1.3.2. <i>Un fichier centralisé est nécessaire pour procéder à un traitement d'identification.....</i>	<i>8</i>
1.4. Si en France les domaines d'utilisation de systèmes biométriques restent circonscrits, une tendance mondiale à leur extension est constatée dans les domaines publics et privés.....	9
1.4.1. <i>Les objectifs ou finalités poursuivis par un système biométrique sont en pratique très variables.....</i>	<i>9</i>
1.4.2. <i>Les cas d'usage de la biométrie dans la vie quotidienne se multiplient.....</i>	<i>10</i>
1.4.3. <i>À l'étranger, les usages de la biométrie à des fins étatiques varient d'un pays à l'autre.....</i>	<i>11</i>
1.5. En France, le recours aux technologies biométriques par la puissance publique à l'échelle de la population nationale est réduit.	12
1.5.1. <i>L'assurance maladie n'utilise jusqu'à présent aucune donnée biométrique, la photographie de la carte Vitale ne permettant pas cet usage</i>	<i>12</i>
1.5.2. <i>Plusieurs fichiers biométriques, d'origine communautaire ou nationale, sont opérationnels pour lutter contre l'immigration illégale.....</i>	<i>14</i>
1.5.3. <i>Le fichier des titres électroniques sécurisés (TES) a connu une mise en place laborieuse.....</i>	<i>15</i>
1.5.4. <i>Pour la population nationale, le fichier TES autorise le traitement de données biométriques dans un but d'authentification uniquement.....</i>	<i>17</i>
1.5.5. <i>Les usages du fichier TES sont réduits à deux cas.....</i>	<i>18</i>
2. À L'ANALYSE, LES INCONVÉNIENTS ET RISQUES INHÉRENTS À LA TECHNOLOGIE L'EMPORTENT SUR LES AVANTAGES RESENTIS À L'USAGE.....	19
2.1. La biométrie présente plusieurs avantages dont ceux d'introduire un degré de sécurité avec une simplicité d'usage et un certain confort.....	19
2.2. La technologie biométrique présente les limites inhérentes à une technologie probabiliste.....	21
2.2.1. <i>L'unicité d'une donnée biométrique n'est pas démontrée.....</i>	<i>21</i>

2.2.2. <i>Les techniques biométriques demeurent approximatives, en raison du taux d'erreur.....</i>	22
2.3. <i>La donnée n'est pas secrète : tout individu laisse derrière lui des traces biologiques.....</i>	24
2.4. <i>Le risque de compromission d'une donnée biométrique, s'il est faible, aurait des conséquences majeures pour les usagers en termes d'accès aux soins</i>	24
2.5. <i>La source de données étant « vivante », la donnée biométrique n'est pas stable dans le temps</i>	25
2.6. <i>Le risque de non-recours et de discrimination en matière d'accès aux soins</i>	26
2.6.1. <i>Il existe un risque de non-recours aux soins non négligeable pour certaines catégories de la population.....</i>	26
2.6.2. <i>Des biais sont possibles liés aux effets d'apprentissage, selon les algorithmes</i>	27
2.7. <i>Le risque de dépendance technologique revêt une importance particulière dans le cadre de la protection des données personnelles.....</i>	27
2.7.1. <i>Les procédures de normalisation des procédés biométriques sont américaines.....</i>	27
2.7.2. <i>Une telle dépendance pourrait être induite par le choix de solutions algorithmiques « propriétaires ».....</i>	28

1. Les cas d'utilisation de la biométrie en France

1.1. De quoi parle-t-on quand on parle de biométrie ?

La biométrie est une notion très large, puisqu'elle englobe un très grand nombre de caractéristiques (cf. 1.1.1). De nombreuses techniques existent au stade expérimental, mais seul un nombre restreint est déployé à l'échelle industrielle (cf. 1.1.2).

1.1.1. La notion de biométrie est très largement définie

Etymologiquement, la biométrie signifie « *la mesure du vivant* ». Elle consiste à vérifier ou déterminer l'identité d'un individu à partir de ses caractéristiques biologiques (comme l'ADN ou le sang), morphologiques (comme l'empreinte digitale, la forme de l'iris ou la forme du visage) ou comportementales (comme la voix, la vitesse de frappe au clavier)¹.

Une caractéristique physiologique, corporelle, ou physique d'un individu n'est toutefois pas en elle-même une donnée biométrique : c'est la mesure d'une caractéristique individuelle qui la rend biométrique et qui permet, par son analyse statistique, d'authentifier et d'identifier cet individu au sein d'une population.

Pour la CNIL, la biométrie est « *l'ensemble des procédés automatisés permettant de reconnaître un individu à partir de la quantification de ses caractéristiques physiques, physiologiques ou comportementales (empreintes digitales, réseau veineux, iris, etc.). Ces caractéristiques sont qualifiées de « données biométriques » par le RGPD², parce qu'elles permettent ou confirment l'identification unique de cette personne* »³.

Encadré 1 : Exemples historiques d'utilisation des caractéristiques biométriques

Les empreintes palmaires étaient déjà utilisées par les scribes égyptiens (aux environs de 3000 av. JC) à des fins d'identification, ou par les Chinois (paume de main encreée, au III^e siècle av. JC), pour authentifier des documents (par un contrôle visuel). C'est au XIX^e siècle, avec la multiplication des registres judiciaires et administratifs qu'une science de l'identification se développe dans plusieurs pays européens, portée en France par l'apparition de la méthode dite du berthillonnage.

Au XX^e siècle, les technologies biométriques se développent concomitamment avec la science informatique qui permet d'automatiser les contrôles biométriques : le contrôle « visuel » se voit substitué par un contrôle s'appuyant sur un processus automatisé, plus rapide et plus fiable. A partir des années 1990-2000, l'essor des nouvelles techniques de l'information et de la communication et les attentats du 11 septembre 2001 donnent une nouvelle impulsion au développement des techniques de reconnaissance biométrique.

Source : Mission d'après Estelle Cherrier. « Authentification biométrique : comment (ré)concilier sécurité, utilisabilité et respect de la vie privée ? Cryptographie et sécurité », Normandie Université, 2021.

¹ ANSSI, « Recommandations relatives à l'authentification multifacteur et aux mots de passe », 8/10/2021.

² Règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données dit règlement général sur la protection des données (RGPD).

³ Source : « Reconnaissance faciale, pour un débat à la hauteur des enjeux », CNIL, 2019.

1.1.2. Si les techniques de biométrie portent sur un nombre foisonnant de caractéristiques, seul un nombre restreint est mis en œuvre de manière opérationnelle

Les progrès technologiques rendent « biométrisables » la plupart de ces caractéristiques biologiques, morphologiques ou comportementales :

- ◆ données biologiques : ADN, sang⁴ ;
- ◆ données morphologiques : dentition, oreilles, iris, rétine, empreinte digitale des mains ou des pieds, empreinte palmaire ou vasculaire de la main, forme du visage, réseau veineux ;
- ◆ données comportementales : son de la voix, écriture, dynamique de frappe au clavier ou de signature, etc.

Pour la plupart, leur mise au point demeure au stade expérimental : lèvres⁵, odeur, chaleur du visage⁶, démarche, peau⁷, etc. Une partie des recherches scientifiques s'intéresse désormais à des modalités biologiques « cachées » : bruit des os⁸, électroencéphalogramme (EEG)⁹, électrocardiogramme (ECG)¹⁰, etc. Ces caractéristiques inhérentes à l'individu présentent en effet l'avantage d'être plus difficilement usurpées, contrairement à d'autres modalités biométriques.

Quelques-unes ont dépassé le stade recherche pour connaître un développement industriel comme les empreintes digitales, la reconnaissance faciale ou l'iris.

Il est par ailleurs tout à fait possible de combiner plusieurs modalités ou facteurs afin de renforcer la sécurité du dispositif d'authentification biométrique tout en minimisant les coûts. Ainsi, en 2017, un groupe de chercheurs a testé un système multi-biométrique d'authentification pour smartphones en combinant la reconnaissance de l'empreinte digitale à l'aide de son capteur intégré et d'un système biométrique comportemental (chemin secret biométrique). Dans le meilleur des cas, la reconnaissance était parfaite sur les bases de données testées et dans le pire des cas, les tests faisaient état d'un taux de fausse acceptation (voir *infra*) inférieur à 2,3%¹¹.

⁴ Plus de 30 systèmes de marqueurs caractérisent le sang de chaque individu.

⁵ Les dents et les lèvres sont des attributs spécifiques connus en médecine légale.

⁶ Technique de la thermographie, au stade expérimental.

⁷ Mesure de la réflexion de la lumière sur la peau, ou biométrie des pores de la peau.

⁸ J. Y. Sim, H. W. Noh, W. Goo, N. Kim, S. -H. Chae and C. -G. Ahn, "Identity Recognition Based on Bioacoustics of Human Body," in *IEEE Transactions on Cybernetics*, vol. 51, no. 5, pp. 2761-2772, May 2021, doi: 10.1109/TCYB.2019.2941281. D'après les chercheurs, la signature spectrale bioacoustique des os est stable dans le temps et permet d'identifier un individu avec un taux de précision de 97,2 % (techniques issues de la sismographie).%

⁹ Voir par exemple le mémoire de maîtrise de Rocio Beatriz Ayala Meza, R. B. (2017). *EEG Biometrics During Sleep and Wakefulness: Performance Optimization and Security Implications*, <https://publications.polymtl.ca/2873/>

¹⁰ Voir par exemple l'article de M. Ingale, R. Cordeiro, S. Thenttu, Y. Park and N. Karimian, "ECG Biometric Authentication: A Comparative Analysis," in *IEEE Access*, vol. 8, pp. 117853-117866, 2020, doi: 10.1109/ACCESS.2020.3004464.

¹¹ Alexandre Ninassi, Sylvain Vernois, Christophe Rosenberger. Authentification multi-biométrique sur mobile respectueuse de la vie privée. 19ème Colloque COmpression et REpresentation des Signaux Audiovisuels (CORESA 2017), Nov 2017, Caen, France.

1.2. La performance des techniques biométriques est variable, mais aucune technique ne présente de garantie absolue

Les différentes techniques biométriques peuvent être évaluées selon une batterie de critères comme l'unicité, la capacité à les collecter ou l'acceptabilité (cf. 1.2.1). Toutefois, parmi les plus répandues, aucune ne donne de garanties sur l'ensemble des critères (cf. 1.2.1).

1.2.1. Les techniques biométriques présentent des caractéristiques différentes

Les techniques de biométrie peuvent être évaluées selon différents critères (cf. tableau 1) :

- ◆ universalité : il s'agit de vérifier si la modalité (objet sur lequel porte la technique biométrique) existe quel que soit l'individu (par exemple, presque toutes les personnes ont un iris, ce qui rend la technique quasi-universelle) ;
- ◆ unicité : il s'agit de vérifier que la mesure de la même modalité sur deux individus ne donnera pas des résultats identiques (par exemple, que deux personnes différentes n'ont pas exactement les mêmes empreintes digitales ou la même voix) ;
- ◆ permanence : il s'agit de vérifier que la mesure de la modalité demeure stable au cours du temps (par exemple, les empreintes digitales peuvent évoluer au cours de la petite enfance) ;
- ◆ collectabilité : il s'agit d'évaluer la facilité d'acquisition, de mesure et d'exploitation de la modalité (par exemple, la collecte de l'empreinte de l'iris est plus complexe que celle de l'empreinte digitale, elle-même plus complexe que celle de la voix) ;
- ◆ performance : il s'agit d'évaluer la robustesse, la fiabilité et la vitesse de collecte et de traitement de la modalité ;
- ◆ acceptabilité : la collecte de la modalité ne doit pas poser de difficulté pour l'utilisateur (caractère plus ou moins intrusif de la collecte). L'acceptabilité est très liée aux facteurs culturels dans lesquels évolue l'individu. En France, la collecte de l'image du visage ou de l'empreinte digitale, répandues par exemple pour déverrouiller les smartphones, sont considérées comme plus acceptables que la collecte de l'image de l'iris, pourtant déployé à très grande échelle en Inde (voir *infra*) ;
- ◆ contournement : il s'agit d'évaluer la difficulté à contourner (voire frauder) le système.

Selon cette grille d'analyse, les caractéristiques des principales techniques biométriques sont regroupées dans le tableau suivant :

Tableau 1 : Propriétés de différentes modalités biométriques

	Universalité	Unicité	Permanence	Collectabilité	Performance	Acceptabilité	Contournement
Iris	***	***	***	**	***	*	***
Rétine	***	***	**	*	***	*	***
ADN	***	***	***	*	***	*	*
Empreintes digitales	**	***	***	**	***	**	***
Paume de la main	**	***	***	**	***	**	***
Réseau vasculaire	**	**	**	**	**	***	***
Oreille	**	**	***	**	**	***	**
Géométrie de la main	**	**	**	***	**	**	**
Visage	***	*	**	***	*	***	*
Démarche	**	*	*	***	*	***	**
Voix	**	*	*	**	*	***	*
Frappe au clavier	*	*	*	**	*	**	**
Signature	*	*	*	***	*	***	*

Source : Mission d'après Estelle Cherrier. « Authentification biométrique : comment (ré)concilier sécurité, utilisabilité et respect de la vie privée ? Cryptographie et sécurité », Normandie Université, 2021.

Les modalités d'authentification par l'iris et la rétine paraissent être celles qui offrent le plus de garanties en termes d'universalité, d'unicité, de permanence temporelle, de performance, accompagnées d'un faible risque de contournement (piratage) : toutefois ces deux techniques pâtissent d'un faible degré d'acceptabilité en raison de leur caractère plus intrusif.

1.2.1. Les principales techniques biométriques sont soit onéreuses, soit peu acceptables, soit sensibles


Les principales modalités biométriques utilisées à grande échelle sont la reconnaissance faciale, les empreintes digitales ou palmaires, le contour de la main, l'iris et, à des fins de recherche criminelle, les empreintes génétiques.

La première opération, pour créer une donnée biométrique, consiste à établir un « *gabarit* », c'est-à-dire les mesures biométriques de l'individu (son « profil biométrique ») qui seront mémorisées et conservées sous une forme permettant son exploitation ultérieure. La prise d'un gabarit lors de l'enrôlement de l'individu est plus ou moins aisée suivant les modalités biométriques, et conditionne la performance du système.

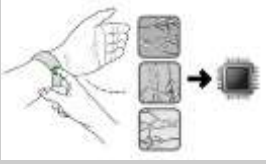
Le tableau 2 ci-après présente les avantages / inconvénients de quelques modalités.

Annexe V

Tableau 2 : Présentation détaillée des modalités biométriques les plus performantes

Modalité	Principes	Avantages	Inconvénients	Domaines d'usage
<p>Empreintes digitales ou dactylographie</p> 	<p>Le dessin de l'empreinte digitale d'un ou plusieurs doigts est enregistré par un capteur ou par encrage sur du papier et scanné. Le nombre de points caractéristiques relevés sur l'empreinte (minuties) varie de quelques dizaines à plus de 100 selon la précision recherchée.</p>	<p>Nombreux travaux scientifiques attestant de la maturité de la technique. Diversité de capteurs, technique très discriminante, très performante, facile à mettre en oeuvre, pas chère, peu vulnérable, peu encombrante.</p> <p>Les dessins papillaires se forment chez le fœtus et proviennent, d'une part, des caractères génétiques et, d'autre part, des mouvements aléatoires du fœtus dans le ventre de sa mère (empreintes différentes même pour les jumeaux). L'empreinte digitale est définie dès le sixième mois de grossesse et ne changera jamais.</p>	<p>Technique pas toujours bien perçue par les utilisateurs car historiquement entachée d'une image « policière ».</p> <p>L'enregistrement se fait par contact, ce qui peut entraîner des réticences d'ordre psychologique ou hygiénique</p> <p>Technique sensible à la température, humidité</p>	<p>À très grande échelle pour des usages liés à la sécurité d'un pays voire d'un continent, ou bien à petite échelle pour des usages domestiques comme l'accès à des objets personnels</p>
<p>Reconnaissance faciale</p>	<p>Le gabarit est basé sur des caractéristiques peu changeantes du visage d'un individu et des distances qui les séparent : écartement des yeux, des arêtes du nez, des commissures des lèvres, des oreilles, du menton, etc.,</p>	<p>Facilité d'utilisation et grande acceptation par le public (démocratisation sur smartphone)</p> <p>Nombreuses solutions existantes sur le marché</p> <p>Preuve du vivant par vidéo disponible pour la majorité des solutions</p>	<p>Sensibilité à l'environnement (luminosité faible, niveau de contraste faible, position du visage)</p> <p>Difficulté de fonctionnement lorsque des accessoires couvrent le visage (lunettes de soleil opaques, masque sanitaire...)</p> <p>-> risque de faux négatifs accru</p>	<p>Possibilité de tromper la solution 2D relativement facilement avec d'une image HD (pour les solutions sans preuve du vivant)</p> <p>La plupart des solutions de reconnaissance faciale associent une preuve du vivant à la capture 2D, basée sur un flux vidéo, pour déjouer les tentatives de contournement.</p>
<p>Iris</p>	<p>Se modifie avec le temps, le dispositif intégrera ces changements dans le gabarit de référence</p>	<p>Technique très discriminante</p> <p>Rapidité du traitement de comparaison à l'usage</p>	<p>Technique ressentie comme intrusive</p>	<p>Technique cantonnée à des usages sans enjeux majeurs de sécurité et concernant un nombre limité d'utilisateurs : accès à des bâtiments privés non stratégiques tels que</p>

Annexe V

Modalité	Principes	Avantages	Inconvénients	Domaines d'usage
				des entreprises, des écoles
Rétine	L'image rétinienne est saisie à l'aide d'une lumière infrarouge dont l'intensité est inoffensive. Un scanner de rétine peut identifier environ 200 points caractéristiques du réseau veineux.	Technique très discriminante et extrêmement difficile à frauder car la rétine est un élément interne du corps	Enregistrement très contraignant car le visage doit rester parfaitement immobile à quelques centimètres du scanner. Technique intrusive souvent mal perçue par les utilisateurs	Technique réservée à certaines applications relevant de la haute sécurité
Paume de la main	La géométrie de la main est scannée : formes, longueurs et épaisseurs des doigts, largeur de la paume... Le nombre de points caractéristiques relevés est d'environ 90.	Simplicité (lecture par scanner biométrique à infrarouge) Méthode biométrique peu intrusive	Technique peu discriminante et sensible aux modifications ou altérations naturelles de la main -accident, vieillissement, arthrose. Lecteur qui peut être encombrant et peu mobile. Ressemblance des caractéristiques entre les individus (en particulier famille proche, jumeaux etc...)	Technique cantonnée à des usages sans enjeux majeurs de sécurité et concernant un nombre limité d'utilisateurs : accès à des bâtiments privés non stratégiques tels que des entreprises, des écoles Fabrication d'un fac-similé relativement aisée (cas du gabarit 2D)
Reconnaissance par les veines	Le schéma du réseau veineux de la main est propre à chaque individu et ne varie pas dans le temps. La main ou le doigt de l'utilisateur est éclairé par des diodes pour enregistrer l'image des veines. Il ne peut être reconnu que du vivant de l'individu, lorsque les globules rouges circulent dans les veines	Technique très fiable et qui ne nécessite pas de contact. Le réseau veineux étant interne, il est très difficile pour un imposteur de le copier 	Technique non encore éprouvée, en particulier à grande échelle, et coûteuse. En 2014, des chercheurs ont développé un bracelet au poignet dont le capteur intégré prend une image des veines, qu'il compare avec celle initialement enregistrée.	Technique peu répandue en Europe, mais déjà utilisée au Japon, notamment par certaines banques. Le réseau veineux remplace le code pour l'authentification. Les données biométriques ne sont pas stockées dans une base mais dans la carte bancaire du client

Source : mission d'après diverses sources, GIE SESAM Vitale, Cité des sciences et de de l'industrie, entretiens.

1.3. Entre identification et authentification, les déterminants de l'architecture d'un système biométrique sont multiples

Les techniques biométriques peuvent être mobilisées à deux fins principales (cf. 1.3.1) :

- ◆ l'authentification de l'identité ;
- ◆ l'identification d'une personne.

Quelle que soit la fin poursuivie, les techniques biométriques peuvent être utilisées (cf. 1.1.2) :

- ◆ lors de l'enrôlement, c'est-à-dire afin d'inscrire une personne dans une base de données ;
- ◆ à l'usage, c'est-à-dire à chaque utilisation du service dont l'accès est contrôlé par biométrie.

Enfin, la question du lieu où est conservé le gabarit biométrique auquel sera confrontée la mesure est structurante pour l'architecture globale d'un système biométrique (cf. 1.3.2).

1.3.1. L'authentification permet simplement de vérifier que l'identité d'une personne est bien celle qu'elle prétend, alors que l'identification est plus intrusive en matière de droits individuels

Un traitement de reconnaissance biométrique permet d'établir ou de s'assurer de l'identité d'un individu par un traitement différentiel entre ce que l'on sait de lui et ce qu'il est, c'est-à-dire qu'il est bien la personne qu'il prétend être. La biométrie est donc une technique adaptée pour lutter contre les usurpations d'identité.

Le traitement biométrique peut revêtir deux natures :

- **le traitement d'identification** consiste à retrouver la donnée biométrique d'un individu parmi une population enregistrée dans une base de données. Il s'agit alors d'une reconnaissance de « 1 » individu parmi « n » individus (symbolisée « 1:n », et appelée « contrôle 1 contre n ») ;
- **le traitement d'authentification** consiste à vérifier que l'individu porteur de la donnée biométrique est bien celui qu'il prétend être. Pour ce faire, on compare la donnée biométrique fournie par l'individu (par exemple en apposant son empreinte sur le lecteur) avec celle qui a été préalablement collectée et stockée (sous la forme d'un « gabarit », par exemple l'empreinte digitale stockée soit localement, soit de manière centralisée – voir *infra*). Si les données correspondent, l'identité alléguée par la personne est exacte. Il s'agit alors de la reconnaissance d'« 1 » individu comparativement à « 1 » enregistrement (symbolisée par « 1:1 » et appelée « contrôle 1 contre 1 »).

Ces traitements peuvent se cumuler afin de sécuriser les données : il est envisageable, à l'enrôlement, de vérifier qu'une empreinte n'est pas déjà présente sous une autre identité (1 : n), puis de limiter à l'usage la biométrie à la seule authentification (1 : 1).

À défaut, si ce traitement d'identification n'est pas réalisé, il existe un risque de détournement de l'identité, dès lors que l'on ne peut pas garantir l'absence de « doublons » (ou de redondance dans la base de données lorsque celle-ci est centralisée - voir *infra*), c'est-à-dire l'existence d'enregistrements multiples dans la base de la même donnée biométrique d'un individu, sous plusieurs identités.

Les contrôles biométriques, par nature intrusifs, peuvent être effectués à chaque usage ou, pour limiter l'atteinte à la vie privée, au seul enrôlement, c'est-à-dire à l'inscription dans la base de données (non nécessairement biométrique : fichier des personnes ayant droit d'accéder à un bâtiment, fichier des bénéficiaires d'un service de rencontre en ligne etc...) donnant accès au service ou au lieu dont l'accès doit être contrôlé.

Annexe V

Dans le domaine régalién, on pourra illustrer ces deux cas d'usage par la carte nationale d'identité électronique (CNIe) ou le passeport :

- ◆ actuellement, les empreintes digitales sont recueillies lors du dépôt de la demande de CNIe. Lors de la remise du document, l'opérateur vérifie que les empreintes digitales contenues dans la carte et celles de la personne venue chercher sa CNIe sont identiques, puis signale la remise de la CNIe qui est alors considérée comme valide dans les fichiers de l'Agence nationale des titres sécurisés (ANTS). Il s'agit ici de biométrie à l'enrôlement, le contrôle des empreintes digitales conditionnant l'inscription de la CNIe dans les bases de données de l'ANTS¹² ;
- ◆ lors du passage des sas PARAFE (voir encadré *infra*), à partir de 2011, les voyageurs munis d'un passeport devaient d'une part le déposer dans une borne de lecture¹³, et d'autre part apposer leur doigt sur le capteur. Si l'empreinte était reconnue, le sas s'ouvre et le passage de la frontière était effectué. Les sas PARAFE de deuxième génération recourent à la reconnaissance faciale, ce qui est également un cas de biométrie à l'usage. Il s'agit là d'un cas de biométrie à l'usage, celle-ci étant mobilisée à chaque passage de la frontière.

Dans le domaine régalién, on pourra illustrer ces deux cas d'usage par la carte nationale d'identité électronique (CNIe) :

- ◆ actuellement, les empreintes digitales sont recueillies lors du dépôt de la demande de CNIe. Lors de la remise du document, l'opérateur vérifie que les empreintes digitales contenues dans la carte et celles de la personne venue chercher sa CNIe sont identiques, puis signale la remise de la CNIe qui est alors considérée comme valide dans les fichiers de l'Agence nationale des titres sécurisés (ANTS). Il s'agit ici de biométrie à l'enrôlement, le contrôle des empreintes digitales conditionnant l'inscription de la CNIe dans les bases de données de l'ANTS ;
- ◆ lors du passage des sas PARAFE (voir encadré *infra*) de première génération, les voyageurs munis d'un document d'identité biométrique devaient d'une part le déposer dans une borne de lecture¹⁴, et d'autre part apposer leur doigt sur le capteur. Si l'empreinte était reconnue, le sas s'ouvrait et le passage de la frontière était effectué. Il s'agit là de biométrie à l'usage, celle-ci étant mobilisée à chaque passage de la frontière. Les sas PARAFE de deuxième génération recourent à la reconnaissance faciale, ce qui est également un cas de biométrie à l'usage.

1.3.2. Un fichier centralisé est nécessaire pour procéder à un traitement d'identification

Comme indiqué *supra*, le contrôle biométrique repose systématiquement sur la comparaison entre un modèle (gabarit) associé à l'identité de la personne d'une part et les caractéristiques de la personne physiquement présente et prétendant avoir cette identité.

La question du lieu de stockage du gabarit se pose donc. Deux architectures principales existent :

¹² Cette fonctionnalité biométrique est optionnelle sur les CNIe (droit d'opting-out de l'utilisateur), contrairement au passeport où elle est obligatoire au-dessus d'un certain âge.

¹³ Bien que le document contienne le gabarit de deux empreintes digitales, elles ne sont pas lues. Cette précaution visait seulement à s'assurer qu'un document d'identité était bien présenté, et que l'accès à la base centralisée était effectué dans le cadre du protocole établi. En effet, les gabarits utilisés dans le cadre du contrôle biométrique étaient issus non du document d'identité mais de la base centralisée opérée par l'ANTS.

¹⁴ L'empreinte digitale de la puce du passeport est comparée à la prise d'empreinte issue du capteur du sas.

- ◆ un **modèle centralisé**, dans lequel une base de données regroupe l'ensemble des gabarits d'une population donnée. C'est par exemple l'architecture qui a été retenue avec la base TES (titres électroniques sécurisés) opérée par l'ANTS, qui regroupe la quasi-totalité¹⁵ des citoyens français disposant d'une CNIe ou un passeport biométrique¹⁶. Ce modèle présente l'avantage de permettre l'identification, mais impose des contraintes importantes en matière de sécurité, la compromission de la base entraînant l'impossibilité de s'authentifier pour l'ensemble des personnes y figurant ;
- ◆ un **modèle centralisé**, dans lequel une base de données regroupe l'ensemble des gabarits d'une population donnée. C'est par exemple l'architecture qui a été retenue avec la base TES (titres électroniques sécurisés) opérée par l'ANTS, qui regroupe la quasi-totalité¹⁷ des citoyens français disposant d'une CNIe ou un passeport biométrique¹⁸. Ce modèle présente l'avantage de permettre l'identification¹⁹, mais impose des contraintes importantes en matière de sécurité ;
- ◆ un **modèle décentralisé**, dans lequel le gabarit est conservé dans un document emporté le plus souvent par la personne devant justifier de son identité. C'est par exemple le cas des cartes bancaires comportant un lecteur d'empreintes digitales intégré à la carte. Cette architecture présente l'avantage de poser des difficultés de sécurité moindres, la compromission d'une carte n'entraînant de difficultés que pour la personne concernée et non pour l'ensemble des utilisateurs du système biométrique.

Il convient de remarquer que la réalisation d'un traitement d'identification requiert la mise en place d'une base de données avec un fichier centralisant l'ensemble des données biométriques d'une population donnée et associées à l'identité de leur propriétaire.

Le cas le plus connu est celui d'une trace biométrique collectée sur une scène de crime, prélevée sur un cadavre inconnu ou une personne amnésique : cette dernière est comparée avec l'ensemble des données biométriques contenues dans une base de référence pour trouver une correspondance, et retrouver l'identité de la personne concernée. Si le traitement échoue, c'est que le propriétaire de la trace biométrique n'est pas référencé dans le fichier.

1.4. Si en France les domaines d'utilisation de systèmes biométriques restent circonscrits, une tendance mondiale à leur extension est constatée dans les domaines publics et privés

Les objectifs ou finalités poursuivis par un système biométrique sont en pratique très variables (cf. 1.4.1). Les techniques biométriques se généralisent dans la vie quotidienne, en particulier pour un usage privé (cf. 1.4.2). À l'étranger, les usages par la puissance publique sont d'intensité et de nature variables d'un État à l'autre (cf. 1.4.3).

1.4.1. Les objectifs ou finalités poursuivis par un système biométrique sont en pratique très variables

Les systèmes biométriques peuvent être mis en œuvre dans des cas d'usage très variés :

¹⁵ 97% des citoyens français sont équipés d'une carte d'identité (source : DMAT).

¹⁶ Dans le cas de la CNIe, il est possible de refuser que les empreintes digitales soient placées dans la base de données. Elles sont alors conservées sur un registre papier (voir *infra*).

¹⁷ 97% des citoyens français sont équipés d'une carte d'identité (source : DMAT).

¹⁸ Dans le cas de la CNIe, il est possible de refuser que les empreintes digitales soient placées dans la base de données. Elles sont alors conservées sur un registre papier (voir *infra*).

¹⁹ Dans le cas de TES, les données sont stockées dans la base centralisée, sans que les outils permettant de faire des traitements d'identification aient été implémentés.

Annexe V

- ◆ à des fins de **recherche criminelle**, dans le cadre notamment de procédures judiciaires. C'est ainsi que les empreintes digitales des personnes mises en cause dans une procédure pénale ou condamnées à des peines de détention sont regroupées dans le fichier automatisé des empreintes digitales (FAED) et que le profil génétique des auteurs d'infraction et des personnes disparues est stocké dans le fichier national automatisé des empreintes génétiques (FNAEG) ;
- ◆ afin de **sécuriser l'accès physique à certains lieux** (site sensible, cantine scolaire...) **ou opérations** (bancaires notamment). L'accès n'est autorisé qu'aux individus dont les données biométriques (empreintes, reconnaissance faciale) sont référencées ;
- ◆ afin **d'authentifier l'identité d'une personne** : c'est par exemple le cas de lors de la délivrance d'une carte nationale d'identité à son titulaire en mairie ;
- ◆ une autre catégorie de traitement (d'authentification uniquement) se développe dans le secteur privé avec l'utilisation de techniques d'évaluation des données biométriques des consommateurs, moins axées sur la recherche de leur identité que **sur leur catégorisation en fonction de caractéristiques spécifiques** (sexe, âge, taille, origine ethnique, orientation sexuelle) **et comportementales** (émotions, traits de personnalité, intentions). De tels traitements sont par exemple être réalisés à des fins publicitaires ou commerciales, ou, par exemple, dans le cadre d'un recrutement, ou encore pour détecter des risques sanitaires (mesure de la température des individus à l'aéroport). Récemment, une application de rencontres en ligne a conditionné l'enregistrement des utilisateurs à la réception d'un selfie vidéo afin d'éviter l'inscription de personnes mineures, ce qui correspond à un usage d'authentification limitée à un trait (l'âge). Les contrôles biométriques peuvent se limiter à l'enrôlement ou être effectués à chaque usage.

Encadré 2 : Le FAED

Le Fichier automatisé des empreintes digitales d'aide à la recherche et à l'identification des auteurs de crimes et de délits ainsi qu'à l'identification de personnes condamnées à une peine privative de liberté. Il permet par ailleurs de faciliter la recherche de personnes disparues ou l'identification de personnes décédées ou grièvement blessées. En 2018, le FAED enregistrait les empreintes de 6,2 millions d'individus, stockées 10, 15 ou 25 ans en fonction de la gravité de l'infraction, de la qualité de mineur ou de majeur de la personne concernée et du caractère national ou international de la procédure.

Source : <https://www.nextinpact.com/article/46338/vers-contrôles-biometriques-en-bord-route>.

1.4.2. Les cas d'usage de la biométrie dans la vie quotidienne se multiplient

La fin du XX^{ème} siècle marque l'essor des technologies biométriques qui se développent concomitamment avec les nouvelles technologies de l'information et de la communication (NTIC). L'automatisation des contrôles biométriques, en substituant à un contrôle « visuel » un contrôle s'appuyant sur un processus automatisé, permet de fiabiliser la technique, de gagner en rapidité et en efficacité. Les attentats du 11 septembre 2001 donnent une nouvelle impulsion mondiale au développement des techniques de reconnaissance biométrique, dans le secteur public comme dans le secteur privé.

Au fil du temps les solutions d'authentification biométriques se sont multipliées dans la vie quotidienne, principalement pour des usages privés. Par exemple, en France, dans les années 2000, l'Aquarium du Grand Lyon et le musée Vulcania en Auvergne ont mis au point une carte de fidélité biométrique anonyme : l'empreinte du pouce suffisait à identifier le titulaire de l'abonnement.

Annexe V

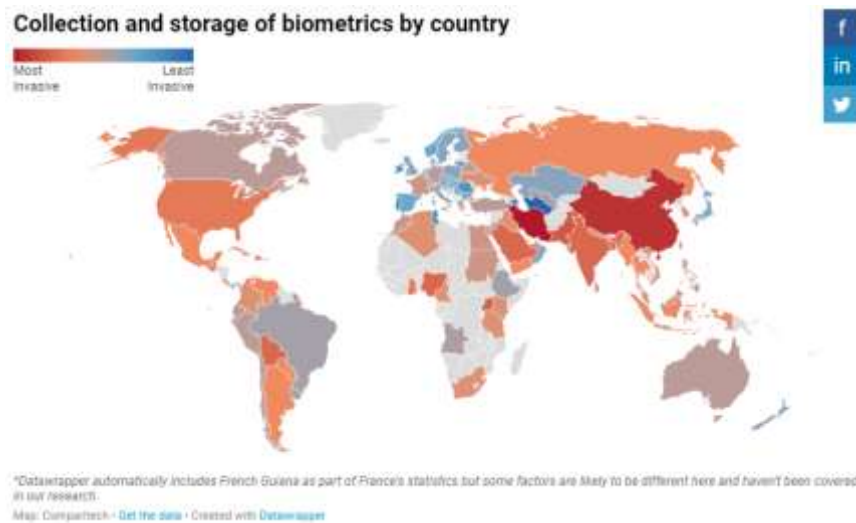
Le procédé biométrique trouve désormais de nombreuses applications dans le domaine domotique (serrures de porte, de fenêtre, casier de piscine²⁰) ou dans le domaine bancaire (carte de paiement, sécurisation des transactions sur internet, distributeur de billets sans carte²¹). Les dernières versions de smartphones embarquent différents procédés biométriques (reconnaissance faciale, empreintes digitales, chemin secret biométrique) pour permettre à leurs propriétaires de les déverrouiller sans avoir à taper un code.

L'utilisation de la biométrie fait désormais partie de la vie courante d'une grande partie des Français familiers des nouvelles technologies. Ainsi, en février 2022 la moitié d'entre eux (47 %) déclaraient utiliser régulièrement la technique d'empreinte digitale. Parmi ceux déclarant utiliser régulièrement au moins une des méthodes biométriques mentionnées, 74 % les utilisaient pour débloquent des appareils (ex. smartphone), et 33 % d'entre eux les utilisaient pour le déverrouillage / la validation d'opérations bancaires²².

1.4.3. À l'étranger, les usages de la biométrie à des fins étatiques varient d'un pays à l'autre

Comme le montre la carte ci-dessous (cf. graphique 1), le déploiement de systèmes biométriques est en voie de généralisation à l'échelle internationale. De nombreux pays stockent et collectent les données biométriques de leurs ressortissants à l'occasion de l'établissement d'un passeport, lors de la délivrance d'un visa ou lors du passage aux frontières.

Graphique 1 : Collecte de données biométriques des citoyens par pays



Source: Biometric data collection by country: What's collected, how is it used? (comparitech.com).

Les systèmes de reconnaissance faciale dans la rue se développent en Grande Bretagne²³, en Chine.

²⁰ Cas d'usage au Brésil.

²¹ Cas du Japon, développé en 2012 après un tremblement de terre.

²² Enquête réalisée par l'entreprise Capterra en février 2022. L'enquête a été envoyée à 1422 participants dont 716 consommateurs ont été sélectionnés pour y participer. Les critères de sélection des participants sont les suivants : résident français, âgé de plus de 18 ans, ayant réalisé une activité en ligne sur les 12 derniers mois.

²³ 73 caméras pour 1000 habitants à Londres, soit une densité comparable à celle de grandes villes chinoises, d'après un article de L'Express : https://www.lexpress.fr/economie/18-000-visages-identifies-par-minute-le-royaume-uni-l-autre-pays-de-la-reconnaissance-faciale_2151210.html

Annexe V

En Inde, l'application de reconnaissance faciale utilisée par la police de New Delhi a permis dans les semaines qui ont suivi son déploiement en 2018 de retrouver sur environ 45 000 enfants, près de 3 000 enfants portés disparus²⁴. L'Inde dispose par ailleurs de la plus grande base de données biométriques au monde : depuis 2009, le système « Aadhaar » attribue un numéro d'identification et stocke les données biométriques (pour chaque personne : dix empreintes digitales, photographie permettant la reconnaissance faciale et deux iris) de 1,3 milliards d'habitants. Dans ce pays, les faux rejets (voir *infra*) peuvent avoir des conséquences dramatiques²⁵ pour les ayants-droits.

Dans au moins deux États de l'Union européenne, certains services de police disposent de smartphones équipés de lecteurs d'empreintes digitales et de dispositifs de reconnaissance faciale (Hambourg²⁶, 2020, Pays Bas, 2011) Par ailleurs, un programme européen prévoit d'équiper la Grèce de scanners biométriques en vue de lutte contre l'immigration clandestine.

Un dispositif de vidéosurveillance algorithmique (15 000 caméras biométriques) a par ailleurs été déployé par le Qatar à l'occasion de la Coupe du monde de football 2022.

1.5. En France, le recours aux technologies biométriques par la puissance publique à l'échelle de la population nationale est réduit.

Si l'assurance maladie ne met pas en œuvre de système biométrique pour ses assurés sociaux, plusieurs fichiers, mis en œuvre et accessibles par les autorités françaises, enregistrent les données biométriques permettant d'authentifier la presque totalité de la population de nationalité française, ainsi qu'une partie des ressortissants résidant sur son territoire :

- ◆ la base EURODAC, contenant les empreintes digitales des demandeurs d'asile et de protection subsidiaire et immigrants illégaux se trouvant sur le territoire de l'UE ;
- ◆ la base VIS (Système d'Information sur les Visas), contenant pour les données photographiques et les empreintes digitales des demandeurs de visa Schengen ;
- ◆ la base de données des titres électroniques sécurisés (TES), contenant les données photographiques et les empreintes digitales de la population de nationalité française à l'occasion de la demande d'établissement de titres sécurisés ;
- ◆ la base de données « SBNA » des étrangers ayant déposé en France une demande de titre de séjour.

1.5.1. L'assurance maladie n'utilise jusqu'à présent aucune donnée biométrique, la photographie de la carte Vitale ne permettant pas cet usage

À sa création en 1997, la carte Vitale ne comprenait pas de photographie.

Un rapport de l'IGAS établi en 2004²⁷, dans son volet concernant les risques de fraude à l'identité, avait considéré trois solutions pour s'assurer de l'identité du porteur de la carte Vitale :

²⁴ [En Inde, une application pour ramener un enfant perdu à ses parents \(francetvinfo.fr\)](https://francetvinfo.fr). (2018)

²⁵ Notamment : "India's all-encompassing ID system holds warnings for the rest of world", Financial times, 11/11/2021; "Of 42 'Hunger-Related' Deaths Since 2017, 25 'Linked to Aadhaar Issues", The Wire, 21/09/2018; "Jharkhand, where not having Aadhaar could starve you to death", The Hindu 9/6/2018.

²⁶ En Allemagne : <https://netzpolitik.org/2021/mobipol-polizei-hamburg-scannt-fingerabdruecke-jetzt-auch-per-handy/>

²⁷ Rapport IGAS n° 2004-066 « Les risques de fraude à l'assurance maladie », établi par Carine Chevrier-Fatome, François Mercereau, Pascal Penaud et Dr Sylvain Picard, juin 2004.

Annexe V

- ◆ généraliser le principe de la présentation de la carte nationale d'identité aux professionnels de santé, pour un coût supplémentaire nul ;
- ◆ apposer une photographie d'identité sur la carte Vitale avec un enrôlement en face à face à l'assurance maladie. Cela représentait un surcoût - évalué par la mission à partir des données de l'assurance maladie et de la DSS - à 160 M€ pour 50 millions de cartes ;
- ◆ apposer une photographie d'identité sur la carte Vitale sans enrôlement en face à face, avec un envoi simple à l'assuré. Cela représentait un coût alors estimé à 35 M€.

La dernière option, recommandée par la mission, consistant en l'apposition d'une photographie sur la carte, dans le but de s'assurer de l'identité de son porteur et de lutter contre la fraude, a été mise en œuvre en 2007 à l'occasion du déploiement d'une nouvelle version de la carte²⁸. À cette occasion, la CNIL, dans son avis²⁹, a pris acte « *que la photographie [portée sur la carte] devra comporter des caractéristiques techniques empêchant une utilisation à des fins de contrôle biométrique et qu'un dispositif de protection empêchera toute copie* ».

Le support physique carte Vitale n'ayant pas de date de fin de validité (contrairement aux droits portés sur la carte - voir l'annexe I sur les cartes Vitale pour une description du parc), environ un tiers du parc actuel se compose de cartes sans photographie, émises entre 1997 et 2007.

Pour celles qui disposent d'une photographie, son utilité paraît en pratique marginale : la quasi-totalité des professionnels de santé interrogés s'accordent sur le fait qu'ils ne regardent que très rarement – voire jamais - la photographie. En effet, le contrôle de la correspondance entre la photo imprimée sur la carte (de petite taille) avec l'apparence de son porteur nécessite, pour le professionnel de santé, de disposer non seulement d'une bonne vue mais de talents de physionomiste voire de clairvoyance, lorsque la carte Vitale comporte une photographie datant de plus de dix ans.

En effet, la qualité de la photographie implantée sur la carte est faible : son degré de définition est bien en deçà de celui permis par la majorité des smartphones actuels. Les standards requis pour la prise de vue ne correspondent pas à ceux exigés pour la délivrance de la carte nationale d'identité ou du passeport (pas de port de lunettes, cou dégagé, visage dégagé des mèches de cheveux, expression faciale neutre...), rendant impossible son exploitation biométrique³⁰.

Il n'en demeure pas moins, comme le souligne une caisse primaire interrogée, qu'une photographie exploitable fait partie des pièces que les assurés peuvent avoir du mal à produire à l'appui de leur demande³¹, ce qui rallonge les délais de fabrication de la carte en question et peut nécessiter un déplacement de l'assuré au guichet. D'après le GIE SESAM Vitale, la photographie est la source des deux premières causes de rejet (problème de détection du visage sur la photo, autre défaut photo – luminosité)³².

²⁸ Cf. il s'agissait d'une recommandation du rapport IGAS n° 2004-066 « Les risques de fraude à l'assurance maladie », établi par Carine Chevrier-Fatome, François Mercereau, Pascal Penaud et Dr Sylvain Picard, juin 2004, dont le coût était évalué à 35 M€.

²⁹ Délibération n° 2007-036 du 20 février 2007 portant avis sur deux projets d'arrêtés relatifs, d'une part, aux spécifications physiques et logiques de la carte d'assurance maladie et aux données y étant contenues et, d'autre part, aux conditions d'émission et de gestion des cartes d'assurance maladie.

³⁰ Conformément à l'avis rendu en 2007 par la CNIL.

³¹ Les rejets sont dus à diverses raisons : photo inexploitable par manque de luminosité, ou floue, comprenant des défauts de cadrage, le port de couvre-chefs, des motifs en arrière-plan, des taches ou des rayures...

³² Source : GIE SESAM Vitale, tableau de bord tous régimes, novembre 2022.

1.5.2. Plusieurs fichiers biométriques, d'origine communautaire ou nationale, sont opérationnels pour lutter contre l'immigration illégale

Depuis deux décennies, la mise en place de fichiers biométriques, initiée par les pays de l'Union européenne et de l'espace Schengen, est portée par l'objectif de contrôle aux frontières et de lutte contre l'immigration illégale :

- ◆ **depuis 2003, le fichier centralisé EURODAC**, créée par l'Union européenne, rassemble les empreintes digitales de l'ensemble des demandeurs d'asile et de protection subsidiaire et immigrants illégaux se trouvant sur le territoire de l'Union, dans le but d'éviter le dépôt par un même demandeur de plusieurs demandes d'asile auprès des différents pays d'accueil³³. Il est procédé à un traitement d'identification des empreintes d'un demandeur à partir des données stockées sur la base³⁴. Fin 2019, 5,59 millions de jeux d'empreintes y étaient enregistrés³⁵ (dont 661 578 à l'initiative de la France, deuxième plus gros contributeur derrière l'Allemagne, et premier pays interrogeant la base, à hauteur de 33% des 300 000 « hits ») ;
- ◆ **depuis 2011, le fichier VIS** (Système d'Information sur les Visa) est une base de données européenne qui centralise l'ensemble des données alphanumériques et biométriques (photographies et empreintes digitales³⁶) des demandes de visa à l'échelle de l'espace Schengen, pour une durée maximale de cinq ans³⁷. Fin 2019, VIS regroupait 69 millions d'empreintes digitales³⁸. En France, l'application VISABIO est consultable par les postes consulaires pour éviter la multiplication des demandes, et par les autorités qui contrôlent le passage aux frontières³⁹ ;
- ◆ **depuis 2017, le système biométrique national (SBNA)** qui est un module additionnel de l'application de gestion des dossiers des ressortissants étrangers en France (AGDREF) les données biométriques liées à un titre de séjour (photographie et empreintes digitales)⁴⁰. Depuis 2019, les forces de l'ordre peuvent théoriquement vérifier, à partir des empreintes digitales d'un étranger sans papier, s'il dispose ou non d'un titre inscrit dans AGDREF⁴¹.

³³ Règlement (UE) n°603/2013 du Parlement européen et du Conseil du 26 juin 2013 relatif à la création d'«Eurodac» pour la comparaison des empreintes digitales aux fins de l'application efficace du règlement (UE) n° 604/2013 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride et relatif aux demandes de comparaison avec les données d'Eurodac présentées par les autorités répressives des États membres et Europol à des fins répressives, et modifiant le règlement (UE) n° 1077/2011 portant création d'une agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (refonte) (JO L 180 du 29.6.2013, p. 1-30).

³⁴ A noter qu'en 2012, le ministère de l'Intérieur recensait un taux de rejet des empreintes digitales d'environ 12% lors de leur dépôt, causé en partie par des altérations volontaires des demandeurs. Source : <https://coordination-asile-cfda.fr/IMG/pdf/cfda20emprei4565.pdf>

³⁵ Source : <https://www.nextinpact.com/article/46338/vers-controles-biometriques-en-bord-route>

³⁶ Relevé des 10 empreintes digitales.

³⁷ Règlement (CE) n°767/2008 concernant le système d'information sur les visas et l'échange de données entre les États membres sur les visas de court séjour (règlement VIS).

³⁸ Source : <https://www.nextinpact.com/article/46338/vers-controles-biometriques-en-bord-route>

³⁹ Elle est aussi consultable par les caisses pour vérification avant ouverture des droits et en cas de suspicion de fraude.

⁴⁰ Relevé des 10 empreintes digitales, 7 millions d'enregistrements en 2017.

⁴¹ Elle est aussi consultable par les caisses primaires pour vérification avant ouverture des droits et en cas de suspicion de fraude.

Depuis 2019, le fichier national d'appui à l'évaluation de la minorité des mineurs (AEM) rassemble les données biométriques des personnes se déclarant mineures en vue de détecter les cas de fraude à la minorité (personnes préalablement identifiées comme majeures dans VISABIO) et éviter la multiplication des demandes de prise en charge au titre de l'aide sociale à l'enfance auprès des conseils départementaux⁴².

Par ailleurs, dans le cadre de leurs travaux en matière de lutte contre l'immigration illégale, les Etats membres de l'Union européenne multiplient les initiatives pour assurer l'interopérabilité des systèmes d'information de sécurité (SIS, Europol, Interpol-SLTD) et de gestion des frontières (EURODAC, VIS, ETIAS, SES, voire ECRIS-TCN) afin de détecter les identités multiples par le nom et/ou l'empreinte digitale⁴³. S'agissant du SIS, les récentes évolutions des textes européens rendent obligatoire le « versement » des données biométriques par l'Etat membre qui fait un signalement dans le SIS, afin de faciliter le repérage des personnes signalées. La France se distingue par sa persistance à ne pas s'y astreindre, ce qui a été signalé à plusieurs reprises lors des évaluations Schengen réalisées par la Commission européenne.

1.5.3. Le fichier des titres électroniques sécurisés (TES) a connu une mise en place laborieuse

La mise en place de la base des titres électroniques sécurisés, créée en 2008⁴⁴ et embarquant des données biométriques de l'ensemble de la ressortissants nationaux, est le fruit d'un long processus :

- ◆ de 2008 jusqu'en 2017, le fichier ne référence que les données biométriques issues des demandeurs de passeports (soit les données biométriques de 15 millions de personnes en 2017). Les données des cartes nationales d'identité étaient alors gérées dans une application obsolète, qui ne permettait pas la numérisation du dossier de demande (lequel contenait notamment la photographie et les empreintes digitales du demandeur), toujours archivé sous format papier ;
- ◆ en 2011, le Conseil d'État juge que « *la collecte et la conservation d'un plus grand nombre d'empreintes digitales que celles figurant dans le composant électronique ne sont ni adéquates, ni pertinentes et apparaissent excessives au regard des finalités du traitement informatisé* », réduisant ainsi de dix à deux le nombre d'empreintes collectées et conservées⁴⁵ ;
- ◆ en 2012, le Conseil constitutionnel censure les dispositions de la loi relative à la protection de l'identité visant à intégrer au TES les données d'une carte nationale d'identité électronique, au motif que le traitement envisagé portait une atteinte à la vie privée disproportionnée au but poursuivi : il aurait permis d'identifier toute personne figurant dans le fichier à partir des données biométriques, notamment ses empreintes digitales, et les données contenues dans le traitement auraient pu être consultées dans certains cas à titre préventif, et non seulement dans un cadre non judiciaire⁴⁶.

⁴² Ce dispositif n'était pas généralisé à l'ensemble des départements en 2021, et son recours par les préfectures demeurait facultatif. 21 000 enregistrements en 2021.

⁴³ <https://www.senat.fr/questions/base/2017/qSEQ170700052.html>

⁴⁴ Décret n° 2008-426 du 30 avril 2008 modifiant le décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques.

⁴⁵ CE, 26 octobre 2011, Association pour la promotion de l'image et autres, n° 317827 et autres.

⁴⁶ Décision n°2012-652DC du 22 mars 2012.

Annexe V

- ◆ en octobre 2016, un décret⁴⁷ autorise la fusion de la base TES existante relative aux passeports et la base des cartes nationales d'identité, dans un but de lutte contre la fraude documentaire et de gestion simplifiée des titres ;
- ◆ à la suite de sa publication, le Conseil national du numérique s'autosaisit et recommande de « *suspendre l'application du décret et les expérimentations en cours* », considérant nécessaire la tenue d'un débat public et l'existence d'alternatives au stockage centralisé de données biométriques⁴⁸. Parallèlement, l'audit de sécurité réalisé par l'ANSSI et la DINSIC⁴⁹ sur le système TES établit que « *les principes de conception du système TES sont compatibles avec la sensibilité des données qu'il contient* ». Toutefois l'audit met en évidence une sécurité globale « *perfectible* » et recommande le durcissement des mesures de sécurité. Il souligne notamment que le caractère unidirectionnel du lien informatique mis en œuvre pour relier les données d'identification alphanumériques aux données biométriques pourrait être détourné et une base de données reconstituée en cas de piratage du lien unidirectionnel existant ;
- ◆ le 30 mars 2017, le fichier TES est déployé sur l'ensemble du territoire. À compter de cette date, les dossiers des CNI numérisés sont également stockés dans le fichier TES, avec les nouvelles demandes ou des renouvellements, soit sur plusieurs années ;
- ◆ dans un arrêt en 2018⁵⁰, le Conseil d'Etat valide la création du fichier TES ;
- ◆ en 2019, un règlement européen⁵¹, applicable à compter du 2 août 2021, impose aux États membres de l'Union européenne le recueil obligatoire des empreintes digitales et l'intégration des données biométriques dans un composant électronique hautement sécurisé de la carte d'identité, à savoir une image numérisée du visage du titulaire de la carte et celle de deux empreintes digitales dans des formats numériques interopérables ;
- ◆ en 2021, un décret⁵² modifie les conditions de recueil des empreintes digitales (article 4-3 du décret n°55-1397 du 22 octobre 1955 instituant la carte nationale d'identité). **Il est désormais possible pour le demandeur de refuser l'enregistrement de ses empreintes dans le fichier TES pour la carte nationale d'identité, qui demeurent conservées et archivées sous format papier**⁵³. En revanche les empreintes demeurent stockées dans la puce de la carte nationale. En outre l'obligation d'enregistrement numérique subsiste pour l'image de la photographie à la fois dans le fichier TES et dans la carte⁵⁴.

⁴⁷ Décret n° 2016-1460 du 28 octobre 2016 autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité.

⁴⁸ Avis rendu en décembre 2016.

⁴⁹ Direction interministérielle du numérique et du système d'information et de communication de l'État.

⁵⁰ Conseil d'État, 10ème - 9ème chambres réunies, 18/10/2018, 404996.

⁵¹ Règlement européen 2019/1157 du 20 juin 2019 relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union et des documents de séjour délivrés aux citoyens de l'Union et aux membres de leur famille exerçant leur droit à la libre circulation.

⁵² Décret n° 2021-279 du 13 mars 2021 portant diverses dispositions relatives à la carte nationale d'identité et au traitement de données à caractère personnel dénommé « titres électroniques sécurisés » (TES).

⁵³ S'agissant des passeports, les usagers ne peuvent en revanche pas s'opposer à la numérisation de l'image de leurs empreintes digitales et à leur enregistrement dans le fichier central.

⁵⁴ Cf. délibération de la CNIL n° 2017-058 du 16 mars 2017 portant avis sur un projet de décret modifiant le décret n° 55-1397 du 22 octobre 1955 instituant la carte nationale d'identité et relatif aux conditions de recueil et de conservation des empreintes digitales du demandeur de carte nationale d'identité.

1.5.4. Pour la population nationale, le fichier TES autorise le traitement de données biométriques dans un but d'authentification uniquement

Plusieurs choix structurants opérés lors de la création du fichier TES ont pour effet de limiter les cas d'usage et *in fine* l'utilité de ce fichier :

- ◆ le fichier TES est interconnecté avec les seuls systèmes d'information Schengen et INTERPOL⁵⁵ ;
- ◆ seules deux empreintes digitales sont conservées, au lieu des dix empreintes conservées initialement (ce qui réduit potentiellement l'intérêt de réquisitions judiciaires, par exemple en cas d'empreintes retrouvées seules et qui pourraient ne pas correspondre à celles relevées dans le cadre d'une enquête judiciaire) ;
- ◆ l'accès au traitement ne peut se faire que par l'identité du porteur du titre d'identité, à l'exclusion, en raison des modalités mêmes de fonctionnement du traitement, de toute recherche à partir des données biométriques elles-mêmes (ce qui rend inopérantes certaines réquisitions judiciaires) ;
- ◆ le traitement ne comporte pas de dispositif de recherche permettant l'identification à partir de l'image numérisée du visage ou de l'image numérisée des empreintes digitales : autrement dit, il n'est pas possible d'identifier un individu parmi la population générale, à partir de ses données biométriques ;
- ◆ un traitement excluant toute opération d'identification : « *le traitement est conçu de manière à rendre impossible l'identification, c'est à dire de rechercher une identité à partir d'une trace biométrique en la comparant à une base de données biométriques* »⁵⁶. Ainsi, à aucun moment, que ce soit lors d'une première demande de titre ou de son renouvellement, il n'est pas procédé à un traitement d'identification des personnes, que ce soit pour un passeport ou une carte nationale d'identité : il est uniquement procédé « *à la comparaison automatique des empreintes digitales de chaque demandeur avec celles précédemment enregistrées sous la même identité, afin de vérifier que l'identité du demandeur de titre est bien celle qu'il prétend avoir (fonction d'authentification des personnes)* »⁵⁷.

⁵⁵ Uniquement pour des informations non nominatives relatives aux numéros des passeports perdus ou volés, au pays émetteur ainsi qu'au caractère vierge ou personnalisé du document.

⁵⁶ Avis Conseil national du numérique fichier TES décembre 2016.

⁵⁷ Délibération de la CNIL n° 2021-022 du 11 février 2021 portant avis sur un projet de décret modifiant le décret n° 55-1397 du 22 octobre 1955 instituant la carte nationale d'identité et le décret no 2016-1460 du 28 octobre 2016 autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité.

Encadré 3 : les limitations induites par l'absence d'identification dans TES

Aucune vérification visant à s'assurer de la présence dans la base de données d'une autre empreinte digitale identique n'est réalisée lors de l'entrée dans le fichier TES d'une biométrie⁵⁸. Il s'agit d'une lacune importante dans la constitution de cette base de données conformément aux règles de l'art en matière de traitements informatiques, dans la mesure où la constitution d'une telle base aurait dû embarquer des mesures visant à assurer la qualité des données et notamment leur intégrité (non redondance).

On ne peut ainsi exclure, si le traitement de dédoublement des empreintes digitales dans le fichier TES était réalisé, de trouver dans ce fichier des correspondances entre empreintes digitales. Qu'un tel traitement ne soit pas réalisé pour le fichier de référence, constitutif de l'identité nationale et dont l'objectif principal est de lutter contre la fraude documentaire, représente une limitation sérieuse.

Par conséquent, faute de traitement d'identification à partir des données biométriques, il n'est pas possible de bénéficier du principal avantage objectif de cette technologie, qui permet, mieux que toute autre facteur inhérent d'authentification, de s'assurer de l'identité unique d'un individu par ce qu'il « est », et non par ce qu'il « connaît » (ex. notoriété ou témoignage de l'identité par un tiers) ou par qu'il « possède » (acte de naissance, ...).

Par ailleurs, la communication électronique des données d'état civil (COMEDDEC) entre les services d'état civil dans les mairies et les services en charge de la délivrance des titres sécurisés, à la date de la mission, est mise en œuvre (et donc sécurise la transmission des données) pour 55 % des nouvelles demandes uniquement⁵⁹. En théorie, il est donc possible qu'un individu dispose de plusieurs véritables titres d'identité sécurisés, établis à partir d'actes d'état civil falsifiés⁶⁰.

Source : Mission.

1.5.5. Les usages du fichier TES sont réduits à deux cas

Le taux d'échec à l'enrôlement des empreintes digitales lors de la demande de CNIe et du passeport électronique est de 0,096 %⁶¹.

Pour la population dont les données biométriques ont été enregistrées, un traitement de comparaison des données biométriques visant à authentifier le porteur d'un titre n'est réalisé que dans un nombre de cas succincts :

- ◆ lors de la remise de la carte nationale d'identité électronique en mairie (technologie des empreintes digitales) ;
- ◆ lors du passage dans les sas du système PARAFE de contrôle aux frontières (technologie de reconnaissance faciale).

⁵⁸ Rapport n° 2019—051-03 [IGF] / 2019-088R [IGAS] / 19089R [IGA], l'identité numérique régaliennne : comment en maximiser le potentiel dans la sphère publique, janvier 2020, page 15 de l'annexe II.

⁵⁹ Source : ANTS.

⁶⁰ En effet, pour les communes non raccordées à COMEDDEC, la falsification des actes d'état civil papier n'apparaît pas d'une grande technicité, au vu de l'accessibilité des technologies et des progrès des technologies numériques (cf. existence de « tutos » sur internet).

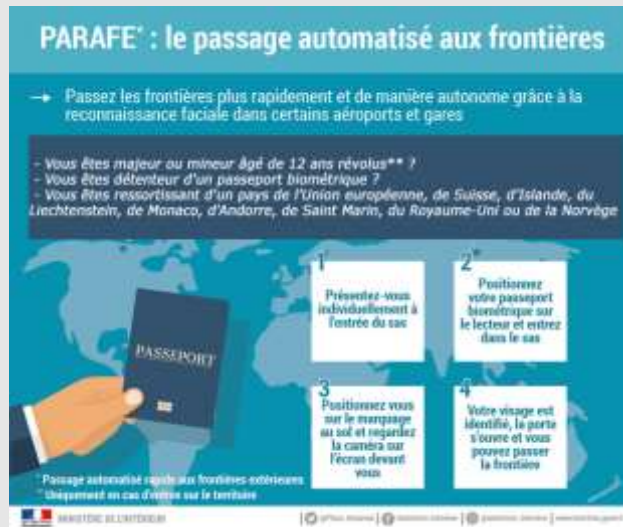
⁶¹ Source : ANTS.

Encadré 4 : Le système PARAFE

Le système PARAFE de contrôle aux frontières automatisé permet de réaliser un contrôle biométrique d'un ressortissant communautaire porteur d'un passeport biométrique, à condition que ce dernier soit volontaire.

Au passage du voyageur dans le sas PARAFE, il est procédé à un traitement d'authentification du gabarit du visage implanté dans la puce du passeport (chiffré) avec le visage du porteur du passeport, ce qui permet de s'assurer de la correspondance entre le porteur du passeport et son titulaire légitime (sauf cas de faux négatifs ou positifs). Techniquement, le gabarit chiffré avec la clé privée du service des passeports est lu après déchiffrement avec la clé publique correspondante par le lecteur biométrique.⁶²

Schéma : description du traitement d'authentification



Source : site internet du ministère de l'Intérieur.

Au 1^{er} août 2022, 222 sas étaient installés sur onze sites. Plus de onze millions de voyageurs les avaient empruntés en 2019⁶³.

Source : Mission.

2. À l'analyse, les inconvénients et risques inhérents à la technologie l'emportent sur les avantages ressentis à l'usage

2.1. La biométrie présente plusieurs avantages dont ceux d'introduire un degré de sécurité avec une simplicité d'usage et un certain confort

La technologie biométrique présente plusieurs avantages :

⁶² <https://www.immigration.interieur.gouv.fr/Europe-et-International/La-circulation-transfrontiere/Le-passage-rapide-aux-frontieres-externes-PARAFE>

⁶³ L'aéroport de Roissy-Charles de Gaulle, l'aéroport d'Orly, la gare du nord et la gare de saint Pancras (Eurostar) , l'aéroport de Lyon, l'aéroport de Marseille , l'aéroport de Nice , l'aéroport de Bâle-Mulhouse , l'aéroport de bordeaux Mérignac , les sites de coquelles et Cheriton (eurotunnel - getlink) , le port de Calais. Source : site du ministère de l'Intérieur

Annexe V

- ◆ sa facilité à l'usage, la rapidité du contrôle, son confort d'utilisation. Tous ces éléments sont toutefois variables d'une technique à l'autre : la reconnaissance faciale peut ainsi être effectuée sans que l'utilisateur ne le remarque⁶⁴, alors que la biométrie oculaire est d'une souplesse d'utilisation beaucoup plus limitée (cf. encadré). De plus, l'enrôlement ou l'usage peuvent être plus ou moins aisés pour l'utilisateur en fonction de la technique mise en œuvre ;
- ◆ le facteur biométrique est insensible à l'oubli, la perte, le vol (et dans une moindre mesure au risque de copie), contrairement à d'autres facteurs d'authentification que sont les codes, clés, carte ou badge d'accès.

Encadré 5 : Le caractère intrusif des biométries oculaires

Parmi les techniques biométriques, les techniques de la mesure de l'œil (iris, rétine), qui permettent de dresser plus de 200 points caractéristiques de l'iris ou du réseau veineux rétinien, sont ressenties comme étant particulièrement intrusives : elles nécessitent un conditionnement proche de celui d'un examen ophtalmologique de type « fond de l'œil ».

La mesure de l'iris est une modalité biométrique très précise, efficace, mais faiblement interopérable. Jusqu'à récemment, le gabarit s'avérait difficile à acquérir : les capteurs de dernière génération ont levé ce frein. Une fois séquencée la signature de l'iris, cette dernière est rapide à contrôler.

Pour les utilisateurs, l'enregistrement demeure contraignant car le visage doit rester parfaitement cadré et immobile lors du séquençage. L'enregistrement du fond de l'œil est souvent moins accepté des utilisateurs, ce qui rend cette technique, à ce stade de développement et de l'avis de l'ensemble des interlocuteurs rencontrés, difficilement généralisable à une population entière.

Source : Mission.

Comme le rappelle l'ANSSI⁶⁵, « l'usage d'un facteur biométrique pour l'authentification, comparé aux autres types de facteurs, présente deux avantages principaux. Le premier est sa **simplicité d'emploi**. En effet, par rapport à un facteur de connaissance il n'y a pas d'information secrète à mémoriser et par rapport à un facteur de possession il n'y a pas d'objet physique à conserver. Dans les deux cas, la biométrie permet de se prémunir des risques liés à l'oubli ou à la perte des moyens d'authentification et d'améliorer l'expérience utilisateur. Le deuxième est **l'authentification directe d'un individu** apportée par la biométrie » au contraire d'une authentification d'un élément secret.

La technologie biométrique est perçue comme étant fiable par la majorité des citoyens⁶⁶ : En effet, « presque 70 % des Français estiment quelles technologies biométriques ne peuvent pas se tromper ou commettre des erreurs. (...) 65 % des Français considèrent que les technologies biométriques sont sûres, dans le sens où elles permettent de collecter et d'utiliser les données personnelles des individus sans risque de piratage ou de mauvaise utilisation ».

Les technologies biométriques, qui se sont invitées dans le quotidien des Français au cours de ces dernières années, par exemple pour déverrouiller leur smartphone, jouissent globalement d'une bonne image. D'après l'enquête réalisée par le Défenseur des droits en octobre 2022, « près des trois quarts des Français voient dans le développement des technologies biométriques et de leurs usages une bonne chose et y associent principalement des traits d'image positifs, les considérant pour plus des deux tiers d'entre deux comme pratiques, efficaces, ou encore fiables. »⁶⁷ En outre, « pour près de trois quarts des répondants, les technologies biométriques seraient considérées comme rigoureuses par la communauté scientifique ».

⁶⁴ Ce qui ne signifie pas pour autant qu'il n'a pas consenti à l'authentification de son identité par ce moyen.

⁶⁵ ANSSI, « Recommandations relatives à l'authentification multi-facteurs et aux mots de passe », 8/10/2021.

⁶⁶ Enquête du Défenseur des droits réalisée en octobre 2022 : « Perception du développement des technologies biométriques en France : entre manque d'information et demande d'encadrement »

⁶⁷ Ibid.

Pourtant, ces dernières qualités attribuées à la biométrie sont discutables en pratique.

2.2. La technologie biométrique présente les limites inhérentes à une technologie probabiliste

La fiabilité de la technique biométrique n'est pas absolue. La confiance ne peut être totale car la fiabilité est obérée par la nécessaire acceptation d'une marge d'erreur, qui même réduite par les avancées de la technologie, demeure incompressible. Dans un système déployé à l'échelle d'une population nationale et à forte fréquence de recours, par exemple pour la sécurisation de la carte Vitale (plus d'un milliard de feuilles de soins électroniques chaque année), il serait donc nécessaire de prévoir des procédures de gestion et de résolution de plusieurs millions d'anomalies (par exemple, 10 millions pour 1 milliard, en prenant un taux d'échec théorique de 1 %).

2.2.1. L'unicité d'une donnée biométrique n'est pas démontrée.

La confiance placée dans la biométrie repose sur la croyance qu'il s'agit d'une technique fiable parce qu'elle permet de mesurer et de restituer la particularité physique (l'unicité) de chaque individu.

En pratique, ce n'est pas le cas. La réalité biologique n'est pas la réalité biométrique : l'unicité d'une donnée biométrique n'a jamais été scientifiquement démontrée⁶⁸.

Les travaux établis à ce sujet concernent la technique des empreintes digitales. Pour les autres techniques, les travaux semblent rares⁶⁹. En 1792, Francis Galton détermina la probabilité que deux personnes aient les mêmes empreintes digitales à une pour 64 milliards. En 1911 les travaux de Victor Balthazard devant l'Académie des Sciences ont établi que le risque de trouver deux personnes ayant 17 points identiques était de 1 sur 17 milliards⁷⁰.

Près d'un siècle plus tard, au début des années 2000, le Government Accountability Office (GAO) aux États-Unis⁷¹ rappelait que cette unicité n'était toujours pas formellement établie et observait qu'aucune recherche n'avait été menée pour vérifier si les empreintes digitales enregistrées dans le fichier du FBI (400 millions d'empreintes) étaient véritablement uniques.

⁶⁸ « La question de l'unicité est importante puisque les systèmes biométriques prétendent relier une donnée à une personne. Elle recouvre en fait deux problèmes : l'unicité du caractère biométrique choisi et l'unicité de la mesure ou de la représentation graphique de ce caractère, l'un comme l'autre devant être propres à une seule personne. Parce que l'unicité d'une donnée biométrique n'a jamais été scientifiquement démontrée, la biométrie repose sur des méthodes statistiques destinées à déterminer la probabilité que deux personnes présentent la même donnée ». Estelle Cherrier. « Authentification biométrique : comment (ré)concilier sécurité, utilisabilité et respect de la vie privée ? Cryptographie et sécurité » [cs.CR]. Normandie Université, 2021.

⁶⁹ La mission n'a pas trouvé de travaux sur d'autres techniques (voix, visage, iris...).

⁷⁰ D'après rapport de l'Assemblée nationale, « les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en œuvre », établi par Christian Cabal, 16 juin 2003.

⁷¹ Organisme d'audit, d'évaluation et d'investigation du Congrès des États-Unis chargé du contrôle des comptes publics du budget fédéral des États-Unis.

2.2.2. Les techniques biométriques demeurent approximatives, en raison du taux d'erreur

Comme toutes les techniques d'évaluation de la mesure, les systèmes biométriques autorisent une marge d'erreur entre la mesure et la référence. La performance technique d'un système biométrique peut être mesurée par différents taux d'erreurs :

- ◆ le taux de fausse acceptation ou faux positifs⁷² (False Acceptance Rate, FAR), qui conduit le système à reconnaître un individu comme légitime alors qu'il ne l'est pas, et à l'accepter à tort. Ces faux positifs ne peuvent pas être détectés en situation réelle : les personnes concernées, qui ont été acceptées à tort, ne cherchent pas à se signaler et demeurent inconnues. Il faut donc, pour évaluer ce taux, procéder à des tests sur une population importante et connue ;
- ◆ le taux de faux rejet ou faux négatifs⁷³ (False Reject Rate, FRR), qui conduit le système à rejeter à tort un individu légitime. Ces faux négatifs peuvent être détectés en situation réelle : les personnes concernées sont bloquées – à tort – par le système, ce qui nécessite une intervention humaine afin de débloquent la situation de ces personnes dès lors qu'elles se sont signalées ;
- ◆ le taux d'échec à l'enrôlement (Failure to Enrol Rate, FER), qui correspond à la proportion de population qui ne parvient pas à s'enrôler⁷⁴ ;
- ◆ le taux de défaut d'acquisition (Failure to Acquire Rate), qui correspond à la proportion d'enregistrements qui se révèlent être d'une qualité insuffisante.

Un système sera d'autant plus sûr que son taux de fausses acceptations est bas. Le problème est que la contrepartie d'un faible taux de faux positifs risque d'être un taux de faux négatifs importants (cf. graphique 2). Pour caricaturer, un système qui refuserait l'accès à toute personne aurait un taux de faux positifs nul et serait totalement sécurisant (personne n'entrerait dans le système sans y être autorisé, puisque personne n'entrerait dans le système), mais un taux de faux négatifs égal à 1 (toutes les personnes qui auraient dû être autorisées à entrer ont été rejetées).

Ainsi, en pratique, pour ne pas bloquer le système, les opérateurs d'un système cherchent le point d'équilibre en fonction, selon l'usage recherché, des taux de faux négatifs limités (lorsqu'il n'est pas acceptable d'exclure des personnes utilisant la biométrie, par exemple pour accéder à la salle VIP d'un aéroport) ou bien des taux de faux positifs faibles (par exemple lors d'un passage automatisé aux frontières, en s'appuyant sur l'existence de contrôles humains classiques pour assurer ce passage). Ces deux taux étant liés, le paramétrage d'un système biométrique est un compromis entre les deux, comme indiqué ci-dessous⁷⁵.

Par exemple, pour les titres sécurisés, le système est paramétré pour minimiser à l'enrôlement le taux de fausses acceptations, et à la délivrance du titre le taux de faux rejet.

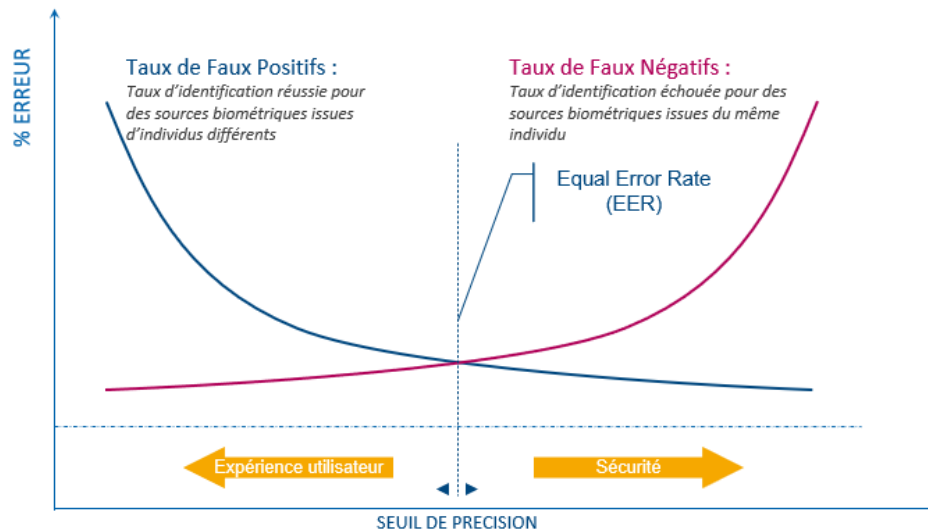
⁷² En statistique, il s'agit de l'erreur de seconde espèce du test statistique pour lequel l'hypothèse nulle est « le gabarit à contrôler et les caractéristiques biométriques présentées sont identiques ».

⁷³ En statistique, il s'agit de l'erreur de première espèce du test statistique pour lequel l'hypothèse nulle est « le gabarit à contrôler et les caractéristiques biométriques présentées sont identiques ».

⁷⁴ Exemple : personnes amputées des deux mains pour les empreintes digitales. La difficulté est ici permanente, mais elle peut être temporaire s'agissant des empreintes digitales lorsqu'on passe d'une atmosphère froide et sèche à une atmosphère chaude et humide.

⁷⁵ Cf. ANSSI, « Recommandations relatives à l'authentification multifacteur et aux mots de passe », 8/10/2021 : « En raison de la nature même de la biométrie, la vérification de l'identité par le vérifieur est probabiliste : un compromis doit toujours être trouvé entre sécurité (maintenir un taux bas de fausse acceptation) et la fonctionnalité (maintenir un taux bas de faux rejet). La qualité de la vérification va aussi dépendre de la qualité du capteur physique utilisé pour mesurer les données biométriques, qui peut varier d'un constructeur à l'autre. (...) ».

Graphique 2 : Marge d'erreur en autorisée en fonction du taux de fausses acceptations et de faux rejets (compromis sécurité / expérience utilisateur)



Source : GIE SESAM Vitale.

Ces taux d'erreur varient, selon les modalités biométriques retenues, selon le degré de précision des capteurs⁷⁶, selon le paramétrage des systèmes (c'est-à-dire la marge d'erreur retenue), et selon les facteurs environnementaux.

En France, en 2010, le ministère de l'intérieur⁷⁷ justifiait le choix de recueillir huit empreintes dans la base centrale des passeports par le fait que les performances des systèmes biométriques à l'enrôlement décroissent avec l'augmentation de la taille de la population de référence : « pour 50 millions d'individus, le taux d'erreur est de 4 % avec 2 doigts et tombe à 0,16 % avec 8 doigts ».

La performance d'un système biométrique peut aussi varier considérablement, en fonction de la marge d'erreur retenue. Ainsi ces dernières années, la presse britannique⁷⁸ s'est régulièrement fait l'écho des mauvais résultats obtenus par le système de reconnaissance faciale mis en place par la police britannique avec, des taux faussés dans plus de 90 % des cas. Il existe un écart entre les performances affichées par les fabricants en matière de reconnaissance faciale lors de tests (taux d'erreur inférieur à 5 %) et les performances constatées en situation réelle.

Surtout, des facteurs exogènes peuvent rendre le système inopérant. Plus l'atmosphère est humide, plus le taux d'erreur lors de la prise d'empreintes augmente. Pire, d'après nos interlocuteurs, en cas de changement brusque de température, par exemple en passant d'un environnement très froid (par exemple, la rue en hiver) à un environnement chaud (par exemple un cabinet médical), la prise d'empreintes serait impossible pendant une dizaine de minutes.

⁷⁶ Les capteurs d'empreintes digitales effectuent une lecture laser tridimensionnelle identifiant l'empreinte externe, interne, les capillaires sanguins, les pores de sudations...

⁷⁷ Rapport Billet, 2010.

⁷⁸ Cf. articles en 2018, 2020 : <https://www.independent.co.uk/news/uk/home-news/met-police-facial-recognition-success-south-wales-trial-home-office-false-positive-a8345036.html>; <https://www.lawfareblog.com/facial-recognition-has-its-eye-uk>

Par ailleurs, s'agissant de taux d'erreur à l'enrôlement, un rapport parlementaire⁷⁹ faisait état en 2006 d'un taux d'erreur de 1 % pour l'iris (pour un temps de vérification réduit de l'ordre de 4 secondes⁸⁰).

2.3. La donnée n'est pas secrète : tout individu laisse derrière lui des traces biologiques

Certaines caractéristiques physiques et biologiques inhérentes à l'individu ne sont pas secrètes et sont assez facilement accessibles et tracées : quotidiennement, toute personne laisse, partout, la trace de ses empreintes digitales⁸¹, de sa voix (sur un répondeur...), la forme de son visage (sur des photographies ou des vidéos...), appose sa signature, etc. Elles ne sont pas confidentielles et ne peuvent pas être protégées contrairement à d'autres facteurs de connaissance ou de possession (mot de passe, badge).

Par ailleurs les travaux présentant des techniques d'usurpation d'identité sont accessibles au grand public et semblent assez facilement reproductibles pour contourner les technologies biométriques, en particulier s'agissant de la dactyloscopie. La fabrication d'une fausse empreinte reproduisant la géométrie du doigt en silicone fait l'objet de nombreux « tutos » sur internet.

L'organisation de hackers « Chaos Computer Club » (CCC) se fait fort de suivre le rythme des progrès technologiques et d'exploiter les failles des technologies biométriques (*spoofing* ou usurpation d'identité) : piratage de l'empreinte du ministre allemand de la défense sur un verre d'eau oublié dans une salle de conférence (2014), piratage de l'empreinte de la présidente de la Commission européenne prise par smartphone lors d'une conférence de presse (2015), piratage de la reconnaissance de l'iris⁸² (2017), piratage), de la reconnaissance par réseau veineux⁸³ (2019), de la reconnaissance faciale vidéo (août 2022).

Dans ses recommandations⁸⁴, l'ANSSI rappelle que la plupart des technologies pour l'authentification biométrique sont sensibles à la contrefaçon (empreintes digitales, reconnaissance faciale, reconnaissance vocale, reconnaissance des veines palmaires, etc.).

2.4. Le risque de compromission d'une donnée biométrique, s'il est faible, aurait des conséquences majeures pour les usagers en termes d'accès aux soins

Le principal désavantage du facteur d'authentification biométrique réside dans son caractère irrévocable, une fois la donnée biométrique compromise.

⁷⁹ Office parlementaire d'évaluation des choix scientifiques et technologiques, compte-rendu de l'audition publique relative à la biométrie, 2006

⁸⁰ La durée d'un traitement d'authentification est désormais inférieur à la seconde, en revanche un traitement d'identification, avec appel à une base centralisée, prend plus de temps, selon l'architecture et la taille de la population.

⁸¹ Ce point a d'ailleurs été soulevé par le Conseil constitutionnel dans sa décision DC 2012-652 du 22 mars 2012 (considérant 10) : « les données biométriques enregistrées dans ce fichier, notamment les empreintes digitales, étant par elles-mêmes susceptibles d'être rapprochées de traces physiques laissées involontairement par la personne ou collectées à son insu, sont particulièrement sensibles ».

⁸² Système d'un smartphone haut de gamme abusé par une simple photographie.

⁸³ En seulement 30 jours, à partir d'un matériel bon marché, deux chercheurs allemands ont réussi à déjouer un système de reconnaissance des veines en fabricant une main en cire.

⁸⁴ Cf. ANSSI, « Recommandations relatives à l'authentification multifacteur et aux mots de passe », 8/10/2021.

Annexe V

En effet, à l'inverse des facteurs d'identification comme les mots de passe ou badges d'accès, qui peuvent être révoqués (c'est-à-dire invalidés et remplacés) s'ils sont perdus ou volés, la caractéristique biologique d'un individu ne peut pas être modifiée : ses empreintes, par exemple, ne pourraient plus être réutilisées en cas de compromission.

Or il n'est pas possible de garantir l'inviolabilité d'un système d'information dans le temps⁸⁵. Comme nous l'ont indiqué certains interlocuteurs de la mission, les bases de données biométriques constituent même des « pots de miel »⁸⁶ pour les hackers.

C'est la raison pour laquelle l'ANSSI recommande de ne pas utiliser un facteur d'authentification inhérent (ex. biométrie) comme unique facteur d'authentification et d'utiliser un tel facteur d'authentification inhérent uniquement en association avec un autre facteur⁸⁷ pour obtenir un niveau d'authentification fort, et associant au facteur biométrique un mécanisme cryptographique conforme au référentiel général de sécurité⁸⁸.

Le risque n'est d'ailleurs pas théorique : ces dernières années, les cas de fuites de bases de données biométriques se sont multipliés, parallèlement au recours accru à ces techniques. Par exemple, en 2019, une faille de sécurité massive dans un système biométrique⁸⁹ utilisé par les banques, la police et les entreprises de défense du Royaume-Uni, a révélé les empreintes digitales de plus d'un million de personnes.

Des travaux récents menés au cours de la dernière décennie sur des technologies biométriques dites « révocables »⁹⁰. Ces technologies consistent à mélanger à la donnée biométrique irrévocable un élément révocable (de type clef, une sorte de diversifiant, que l'on pourra renouveler en cas de compromission de ces fameuses données de référence) pour créer des pseudo-identités pouvant être révoquées en cas de compromission. D'après les experts consultés par la mission, ces technologies relèvent à ce stade plus de travaux de recherche que de solutions éprouvées et praticables⁹¹.

2.5. La source de données étant « vivante », la donnée biométrique n'est pas stable dans le temps

Tout organisme vivant s'adapte à son environnement et au rythme des évolutions biologiques : il vieillit, subit des traumatismes plus ou moins importants, ce qui change la mesure biométrique et nécessite son actualisation. Le renouvellement du gabarit biométrique de référence est donc nécessaire pour éviter l'augmentation des taux d'erreur. La qualité de la comparaison de la donnée biométrique se dégrade à plus ou moins long terme.

⁸⁵ Comme le rappelle l'audit ANSSI/DINSIC relatif au système TES⁸⁵, 17 janvier 2017, « il est impossible de garantir l'inviolabilité absolue d'un système d'information dans le temps. La question de la sécurité (...) renvoie à l'arbitrage que doit faire l'État en matière d'acceptation des risques résiduels inévitables liés à la mise en œuvre de ce système, au regard des bénéfices escomptés, (...) comme c'est le cas pour tout système d'information, quelle que soit sa sensibilité ».

⁸⁶ Propos issu des entretiens.

⁸⁷ Qui ne sera pas forcément biométrique, par exemple un mot de passe, un code pin, une question secrète, ou la détention d'un appareil tels qu'un smartphone...

⁸⁸ Pris en application du décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives.

⁸⁹ Système de la société sud-coréenne Suprema qui se présentait comme « le leader du marché européen des systèmes de contrôle d'accès basés sur des données biométriques ».

⁹⁰ Exemple : projet européen TURBINE (TrUsted Revocable Biometric IdeNtitiEs), mené dans le cadre du 7e Programme Cadre de Recherche et le Développement de l'Union Européenne.

⁹¹ Thèse de Mohamed Amine Hmani : « utilisation des données biométriques pour la régénération des clés cryptobiométriques révocables », novembre 2022.

Annexe V

Ainsi, pour les empreintes digitales, le taux d'erreur enregistré lors du retrait d'un titre sécurisé est inférieur à 1% pour les adultes, mais grimpe à 25 % lors de la demande de renouvellement d'un titre sécurisé⁹². Quoique les empreintes soient beaucoup plus résilientes que le visage, et plus difficiles à usurper ou imiter, il demeure un taux significatif d'échec de la comparaison. Aussi, s'agissant de reconnaissance faciale, l'ANTS évoque une périodicité de 5 ans pour renouveler le gabarit du visage⁹³.

De plus, l'usage de la biométrie, pour certaines catégories de personnes n'est tout simplement pas possible du fait de leur handicap ou de leurs caractéristiques physiologiques, par exemple pour les empreintes digitales :

- ◆ les services d'état civil font état de difficultés à prendre les empreintes digitales des personnes âgées, la peau se détériorant naturellement avec l'âge⁹⁴ ;
- ◆ c'est également le cas pour les personnes qui ont la peau qui pèle, rendant impossible la reconnaissance digitale, tout comme celles dont la transpiration est excessive⁹⁵ ;
- ◆ même constat pour la population dont les doigts présentent des microcoupures (jardiniers, bricoleurs, travailleurs manuels...) ;

S'agissant des biométries oculaires, certaines pathologies peuvent faire changer l'iris de couleur.

Pour toutes ces populations, le déploiement d'un système biométrique induit potentiellement un risque de non-recours ou de discrimination en matière d'accès aux soins⁹⁶.

2.6. Le risque de non-recours et de discrimination en matière d'accès aux soins

2.6.1. Il existe un risque de non-recours aux soins non négligeable pour certaines catégories de la population

Le Défenseur des droits alerte sur l'effet potentiellement dissuasif des technologies biométriques pour l'exercice de droits fondamentaux comme la liberté d'expression, d'aller et venir, d'assemblée, d'association, et, plus largement, l'accès aux droits. Il évoque également un risque d'exclusion, en particulier pour les personnes issues de groupes discriminés comme les étrangers⁹⁷. Il note qu'ils pourraient renoncer à des soins de santé auxquels ils ont pourtant droit, de peur d'être identifiés comme étant en situation irrégulière. La sensibilité de certains usagers sur ces questions – par ailleurs dans l'incapacité d'engager des frais de santé – a été rapportée à la mission par un centre hospitalier.

⁹² Source : ANTS.

⁹³ 10 ans pour certains industriels rencontrés par la mission : ceci paraît être un maximum, les caractéristiques biométriques d'un visage peuvent être altérées rapidement (prise de poids, maladie...).

⁹⁴ Ce risque diminue avec la prise de plusieurs empreintes.

⁹⁵ La température des doigts est irrégulière : entre 8 à 10°C au-dessus de la moyenne ambiante.

⁹⁶ En Inde, plusieurs décès sont documentés directement liés aux dysfonctionnements du système biométrique AadhaarAadhar.

⁹⁷ Cf. enquête du Défenseur des droits réalisée en octobre 2022 : « Perception du développement des technologies biométriques en France : entre manque d'information et demande d'encadrement ».

2.6.2. Des biais sont possibles liés aux effets d'apprentissage, selon les algorithmes

La mise au point des algorithmes utilisés par les logiciels de reconnaissance biométrique repose sur un échantillon de données d'entraînement ou d'apprentissage, dont l'origine n'est pas toujours connue. Les travaux de validation de ces algorithmes et des systèmes biométriques sont restés jusqu'à présent assez peu nombreux et peu transparents⁹⁸.

Les systèmes biométriques de reconnaissance faciale seraient plus performants pour reconnaître un homme, de type caucasien, qu'une femme à la peau de carnation plus foncée. Ainsi, dans une étude parue en 2019, le National Institute for Standards and Technology (NIST) a trouvé que la majorité des 189 algorithmes de reconnaissance faciale étaient biaisés, et s'avéraient moins précis pour les populations issues de minorités ethniques et raciales⁹⁹.

Un rapport du Sénat souligne la nécessité de mieux assurer la traçabilité des données d'apprentissage non seulement pour des enjeux régaliens, mais également pour éviter des biais de fonctionnement du système biométrique¹⁰⁰.

2.7. Le risque de dépendance technologique revêt une importance particulière dans le cadre de la protection des données personnelles

La mise en œuvre de technologies biométriques expose à une double dépendance :

- ◆ une dépendance aux normes, aujourd'hui américaines ;
- ◆ une dépendance aux solutions algorithmiques développées par les industriels.

Par ailleurs, comme toute activité industrielle, le secteur de la biométrie dépend de ses fournisseurs, avec par exemple la disponibilité mondiale des composants, par exemple lorsqu'il s'agit de fabriquer/renouveler des cartes embarquant des lecteurs d'empreintes, à grande échelle (la même problématique n'étant toutefois pas spécifique au secteur de la biométrie).

2.7.1. Les procédures de normalisation des procédés biométriques sont américaines.

Il n'existe pas de dispositif de labellisation ou de certification européen. Le National Institute for Standards and Technology (NIST) américain, dépendant du FBI, dispose d'un monopole de fait sur le marché international de la standardisation des technologies biométriques. Faute de standards européens, les critères d'évaluation établis par le NIST sont largement utilisés dans le monde, y compris au sein des appels d'offres européens. L'IN Groupe rapporte par exemple le cas d'un capteur d'empreintes que le NIST a refusé de qualifier.

⁹⁸ Cf. Bernadette Dorizzi, directrice de recherche et des formations doctorales de Télécom SudParis, ex-coordinatrice du réseau européen BioSecure.

⁹⁹ National Institute of Standards and Technology Interagency or Internal Report 8280, Natl. Inst. Stand. Technol. Interag. Intern. Rep. 8280, 81 pages (December 2019).

¹⁰⁰ Cf. rapport d'information du Sénat n°627 (2021-2022): « La reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », établi par Marc-Philippe DAUBRESSE, Arnaud de BELENET et Jérôme DURAIN, qui recommande notamment la création d'un dispositif de labellisation des logiciels de reconnaissance biométrique.

2.7.2. Une telle dépendance pourrait être induite par le choix de solutions algorithmiques « propriétaires »

Plusieurs interlocuteurs de la mission ont souligné le risque de dépendance technologique du fait des choix matériels et de développements logiciels opérés à la fois pour la capture des gabarits et pour la lecture des données biométriques. Ce risque de dépendance vaut pour le développement de tous les systèmes d'information, mais devrait être considéré avec une acuité particulière s'agissant de systèmes biométriques.

Schématiquement, si la donnée biométrique est stockée à plat (« flat »), il est possible de conserver la maîtrise du gabarit, dès lors qu'il est possible de recréer ou de modifier l'algorithme de capture du gabarit (par exemple, en cas de compromission) ou le traitement permettant la lecture de la donnée biométrique : le gabarit n'est pas « propriétaire ». Si la donnée biométrique n'est pas stockée à plat mais uniquement sous la forme d'un gabarit, il n'est pas possible de conserver son indépendance vis-à-vis du concepteur, sauf à choisir de refondre le système biométrique dans son ensemble, par exemple en cas de compromission, ou en cas de remise en concurrence (algorithmes de capture et de lecture).

Le même raisonnement vaut pour l'algorithme de lecture, qui va lire la donnée biométrique présentée et la comparer avec le gabarit enregistré. Le dernier niveau de dépendance technologique est matériel. D'après IN Groupe, conserver la maîtrise des logiciels (et donc des algorithmes) permet d'assurer l'interopérabilité des capteurs. Par ailleurs la fabrication des cartes embarquant des lecteurs d'empreintes, à grande échelle (soit en théorie de l'ordre de 58 millions qui est le nombre de carte Vitale valides à date) pose la question de la disponibilité mondiale des composants.

ANNEXE VI

Scénarios d'une carte Vitale biométrique

SOMMAIRE

1. ... LES SCÉNARIOS BIOMÉTRIQUES ENVISAGEABLES SONT CONTRAINTS	1
1.1. L'architecture retenue ne peut pas être centralisée.....	1
1.1.1..... <i>Sans même examiner les sujets juridiques, la base centralisée pose des problèmes techniques majeurs.....</i>	3
1.1.2..... <i>La technologie embarquée apparaît plus praticable</i>	4
1.2. La fréquence d'usage envisagée est également structurante	5
1.2.1..... <i>L'appréciation des professionnels de santé libéraux.....</i>	5
1.2.2..... <i>En établissement, une préoccupation plus liée à l'identitovigilance qu'à la fraude.....</i>	8
1.2.3..... <i>La fréquence d'un contrôle biométrique pourrait être réservée aux situations les plus critiques en termes de risques de fraude.....</i>	9
1.3. Le recueil de la donnée biométrique à l'enrôlement lors d'une demande d'une carte Vitale	10
1.3.1..... <i>La procédure actuelle de remise de la carte Vitale est simple mais apparaît robuste.....</i>	10
1.3.2..... <i>La mise en place d'un contrôle biométrique nécessiterait de recueillir les données biométriques des assurés sociaux.....</i>	10
1.3.3..... <i>Le coût en ETP supplémentaires du seul enrôlement en face à face s'élèverait à plusieurs centaines de millions d'euros chaque année</i>	11
1.3.3.1..... <i>L'actualisation de l'estimation effectuée dans le cadre de la mission de l'IGAS de 2004 aboutirait à un coût annuel de 240 M€.....</i>	12
1.3.3.2..... <i>L'estimation de la CNAM s'établit aux alentours de 300 M€.....</i>	12
1.3.3.3..... <i>La mission estime que le coût en ETP d'un enrôlement biométrique des assurés sociaux serait de l'ordre de 535 M€, tout en étant très dépendant de la fréquence de renouvellement du stock de cartes Vitale biométriques ...</i>	12
1.3.4..... <i>L'enrôlement biométrique pourrait voir son coût réduit s'il se faisait à distance</i>	14
1.4. L'empreinte digitale et la reconnaissance faciale sont, en France, mieux acceptées que la reconnaissance de l'iris	15
1.4.1..... <i>Certaines modalités biométriques sont désormais utilisées à grande échelle</i>	15
1.4.2..... <i>Des modalités biométriques bénéficient d'une bonne acceptation dans la population française</i>	15
1.4.3..... <i>Les deux modalités à forte acceptabilité, empreinte digitale et reconnaissance faciale, présentent des performances éprouvées sous réserve d'un compromis à trouver entre expérience utilisateur et niveau de sécurité.....</i>	17
2. ... LA MISSION A PLUS PARTICULIÈREMENT ÉVALUÉ DEUX SOLUTIONS EMBARQUÉES UTILISANT LES EMPREINTES DIGITALES OU LA RECONNAISSANCE FACIALE.....	18
2.1. La reconnaissance des empreintes digitales, outre un surcoût significatif par rapport à la situation actuelle, risque de faire apparaître un nombre important de faux négatifs	18
2.1.1..... <i>Le gabarit des minuties des doigts est stocké sur la carte Vitale.....</i>	18
2.1.2..... <i>La large diffusion de la solution risque de mettre en évidence un nombre important d'échecs à l'usage.....</i>	19

2.1.3.....	<i>La solution biométrique engendrerait des coûts de production entre deux et 10 fois supérieurs à la solution actuelle.....</i>	19
2.2.	La reconnaissance faciale est probablement moins onéreuse mais n'offre pas de garanties en termes de faux négatifs	21
2.2.1.....	<i>Une photographie de haute résolution ou un gabarit des traits du visage sont stockés en carte</i>	21
2.2.2.....	<i>La reconnaissance faciale engendre aussi un nombre important de faux négatifs pour un usage massif, tout en étant très sensible aux conditions d'acquisition du gabarit</i>	21
2.2.3.....	<i>Les surcoûts liés à cette technique apparaissent plus limités que la technique biométrique.....</i>	21
2.3.	Les coûts liés au déploiement d'une carte Vitale biométrique sont de l'ordre de 1 milliard d'euros.....	22
2.3.1.....	<i>La mission n'a pas pu évaluer les coûts de développement</i>	22
2.3.2.....	<i>Au total, la solution biométrique apparaît très onéreuse.....</i>	22
2.4.	Le recours à la biométrie ne peut s'envisager sans mettre en place de solution alternative, en cas notamment de faux négatif	27
2.4.1.....	<i>Un système alternatif doit permettre l'accès aux droits garantis par l'assurance maladie.....</i>	27
2.4.2.....	<i>La nécessité de mettre en place une procédure d'alerte de l'assurance maladie pour traiter les cas de rejets (positifs ou négatifs)</i>	28
2.4.3.....	<i>La question de la personne sur laquelle le risque repose en cas de faux négatif (rejet injustifié) doit être tranchée.....</i>	28
2.5.	En conclusion, la mise en place d'une carte Vitale biométrique serait onéreuse tout en ne présentant, en raison des spécificités de l'assurance maladie, que peu de garanties	29

3. ... UNE ALTERNATIVE AUX SCÉNARIOS BIOMÉTRIQUES : LE SUPPORT DE LA CNIÉ ET DU TITRE DE SÉJOUR..... 30

3.1.	L'utilisation de la carte nationale d'identité en substitution de la carte Vitale permet d'additionner les gains dans les domaines de la lutte contre la fraude et de l'identitovigilance.....	31
3.2.	L'adoption de la solution « NIR sur CNIé » permettrait de simplifier la situation des enfants mineurs, source de difficultés rapportés par l'ensemble de nos interlocuteurs	32
3.3.	La quasi-totalité de la population vivant en France disposera à terme d'un titre électronique sécurisé.....	33
3.4.	D'autres pays, notamment européens utilisent le support de la carte d'identité comme clé d'accès aux droits de l'assurance maladie	35
3.4.1.....	<i>Portugal</i>	35
3.4.2.....	<i>Danemark.....</i>	35
3.4.3.....	<i>Belgique.....</i>	36
3.4.4.....	<i>Suède.....</i>	36
3.4.5.....	<i>Allemagne.....</i>	37
3.4.6.....	<i>Espagne.....</i>	38
3.4.7.....	<i>États Unis.....</i>	38
3.5.	Le NIR pourrait être embarqué sur la CNIé et les titres de séjour	39
3.5.1.....	<i>La CNIé pourrait disposer d'un container dans sa puce permettant de communiquer le NIR aux professionnels de santé.....</i>	39
3.5.2.....	<i>La CNIé pourrait afficher le NIR dans le 2D-DOC présent à son verso</i>	40
3.5.3.....	<i>Le NIR devrait être traité par l'Imprimerie nationale de manière sécurisée.....</i>	41

3.6. Les téléservices de consultation des droits doivent être fiables et disponibles .	42
3.7. La CNIe ou le titre de séjour devrait permettre, dans ce scénario, la signature de feuilles de soin électroniques.....	44
3.8. La montée en charge du déploiement de la solution CNIe sera liée au renouvellement et à la mise à niveau du parc de cartes d'identité	44
3.9. Les professionnels de santé et établissements de santé interrogés sont favorables : ils y voient une source de simplification administrative et de sécurisation des soins	44
3.10.. La CNAM a émis de très fortes réserves, qui paraissent pouvoir être levées ...	45
3.11.. Les conditions pré-requises à la réalisation d'un tel scénario, listées par la CNIL, paraissent pouvoir être remplies, sous réserve d'une étude approfondie.	46

1. Les scénarios biométriques envisageables sont contraints

La mise en place d'une carte Vitale biométrique nécessite de répondre à plusieurs questions :

- ◆ quelle architecture retenir, celle d'une base centralisée ou d'une biométrie décentralisée ? ;
- ◆ quelle est la fréquence de la vérification de l'identité par l'usage de la biométrie ?

1.1. L'architecture retenue ne peut pas être centralisée

Deux familles principales d'architecture existent :

- ◆ la mise en place d'une base centralisée regroupant l'ensemble des gabarits biométriques des assurés sociaux (cf. 1.1.1) ;
- ◆ la mise en place d'une architecture décentralisée, les gabarits biométriques étant alors gardés par l'assuré social lui-même (cf. 1.1.2).

La première opération, pour créer une donnée biométrique, consiste à établir un « **gabarit** », c'est-à-dire les mesures biométriques de l'individu (son « profil biométrique ») qui seront mémorisées et conservées sous une forme permettant son exploitation ultérieure.

Les gabarits biométriques d'une population, c'est-à-dire les données biométriques qui servent de référence pour authentifier les porteurs de la carte, peuvent être stockés « localement » et uniquement dans la carte Vitale du titulaire (« biométrie sur carte ») et/ ou dans une base de données centralisée. Une telle architecture, dite centralisée, permet d'opérer, en sus de l'authentification, l'identification d'un gabarit par comparaison de ceux en base¹, et de s'assurer qu'un individu ne dispose pas de plusieurs cartes.

Seul un traitement d'identification couplé à un traitement d'authentification permet en réalité d'écarter le risque de fraude (cf. encadré 1).

¹ Un tel traitement est opéré via un système d'identification biométrique automatique (AFIS), qui permet d'exploiter la base.

Encadré 1 : Les traitements à l'authentification et à l'identification

Le traitement d'identification consiste à retrouver la donnée biométrique d'un individu parmi une population enregistrée dans une base de données. Il s'agit alors d'une reconnaissance de « 1 » individu parmi « n » individus (symbolisé « 1:n », et appelée « dit « contrôle 1 contre n » ») ;»

Le traitement d'authentification consiste à vérifier que l'individu porteur de la donnée biométrique est bien celui qu'il prétend être. Pour ce faire, on compare la donnée biométrique fournie par l'individu (par exemple en apposant son empreinte sur le lecteur) avec celle qui a été préalablement collectée et stockée (sous la forme d'un « gabarit », par exemple empreinte digitale stockée soit localement, soit de manière centralisée – voir *infra*). Si les données correspondent, l'identité alléguée par la personne est exacte. Il s'agit alors de la reconnaissance d'« 1 » individu comparativement à « 1 » enregistrement (symbolisée par « 1:1 » et appelée « dit « contrôle 1 contre 1 » »).

Ces traitements peuvent se cumuler afin de sécuriser les données : il est envisageable, à l'enrôlement, de vérifier qu'une empreinte n'est pas déjà présente sous une autre identité (identification 1 : n), puis de limiter l'usage biométrique à la seule authentification (1 : 1).

À défaut, si ce traitement d'identification n'est pas réalisé, il existe un risque de détournement de l'identité, dès lors que l'on ne peut pas garantir l'absence de « doublons » (ou de redondance dans la base de données lorsque celle-ci est centralisée - voir *infra*), c'est-à-dire l'existence d'enregistrements multiples dans la base de la même donnée biométrique d'un individu, sous plusieurs identités.

Source : Mission.

En croisant la fréquence du traitement biométrique à l'architecture retenue (donnée stockée sur la carte/centralisée en base), on obtient des scénarios plus ou moins risqués et attentatoires aux libertés et plus ou moins préventifs en matière de lutte contre la fraude (cas A, B, C, D ci-dessous) :

- ◆ le cas A permet de sécuriser uniquement la procédure de délivrance au porteur ;
- ◆ le cas D généralise le recours à la biométrie et permet de s'assurer à la fois qu'un individu ne dispose que d'une seule carte, qui ne peut être utilisée que par lui.

Tableau 1 : Traitements biométriques possibles pour une carte Vitale biométrique selon l'architecture et la fréquence retenues

Efficacité en matière de lutte contre la fraude (de + à ++++)		Fréquence du traitement biométrique	
		A l'enrôlement (lors de la création de la carte)	A chaque utilisation de la carte vitale chez un professionnel de santé
Architecture du traitement biométrique	Le gabarit biométrique est uniquement stocké sur la carte physique sur un mode décentralisé	CAS A (+) Un traitement est opéré à l'enrôlement uniquement ce qui permet d'authentifier que le détenteur de la carte est bien son bénéficiaire.	CAS B (++) Outre le traitement à l'enrôlement, un traitement d'authentification est opéré à chaque passage chez un professionnel de santé pour s'assurer que le porteur de la carte est le bénéficiaire.
	Le gabarit biométrique est stocké dans une base centralisée (éventuellement anonymisée)	CAS C (+++) Outre un traitement d'authentification, un traitement d'identification est opéré une fois à l'enrôlement pour vérifier qu'à une empreinte ne correspond qu'un seul individu	CAS D (++++) Outre le traitement d'identification à l'enrôlement, un traitement d'authentification avec recherche dans la base est opéré à chaque passage chez un professionnel de santé.

Source : Mission.

1.1.1. Sans même examiner les sujets juridiques, la base centralisée pose des problèmes techniques majeurs

La création d'une base centralisée stockant les données biométriques (photographies et/ou empreintes digitales) revient à créer un fichier similaire à celui établi pour les titres électroniques sécurisés (fichier TES), mais qui serait spécifiquement utilisé par l'Assurance maladie.

Une telle base permettrait de réaliser :

- ◆ soit un traitement à l'identification uniquement pour l'enrôlement (fréquence du traitement réduit à la première demande et au renouvellement de la carte) ;
- ◆ soit la réalisation d'un traitement d'identification à l'enrôlement et un traitement d'authentification lors de l'utilisation de la carte chez le professionnel de santé (soit une augmentation de la fréquence des traitements : lors de la première demande de carte, son renouvellement, et lors du passage chez un professionnel ou en établissement de santé- utilisation systématique, aléatoire, ou fréquence à déterminer).

A la connaissance de la mission et des conseillers sociaux interrogés, aucun pays européen ne s'est doté, à la date de la mission, de base de données biométriques centralisée ayant pour finalité de lutter contre la fraude à l'accès aux soins.

Très peu de pays européens ont fait d'ailleurs ce choix d'architecture, y compris pour délivrer une carte d'identité biométrique sécurisée (Espagne, Pays Bas, la Lituanie²).

Comme on l'a vu *supra*, utiliser le contenu du fichier TES pour créer une base biométrique « bis » à d'autres finalités est exclu (indépendamment même des considérations juridiques³) techniquement :

- ◆ il n'est pas possible d'accéder au fichier autrement que par un réseau privatif sécurisé de liaisons dédiées (pas d'accès internet)⁴ ;
- ◆ les données sont chiffrées et seule une autorité habilitée peut accéder aux empreintes de la puce, qui s'authentifie de manière « forte » ;
- ◆ le fichier est ainsi construit qu'il n'est pas possible d'interroger la base à partir des empreintes pour retrouver l'identité (lien unidirectionnel chiffré qui unit le compartiment de l'application contenant les éléments alphanumériques au compartiment contenant les données biométriques) ;
- ◆ les connexions sont mesurées et contingentées, de même que le nombre de déchiffrements pour éviter les traitements de masse.

Ces mesures de sécurité ont été imposées notamment par l'ANSSI du fait des risques d'attaque de la base. Comme le rappelle le Conseil national du numérique, « **une base centrale ne peut être totalement sécurisée. Quelles que soient les garanties juridiques et techniques apportées, la création d'un dispositif centralisé de cette taille n'est jamais totalement exempte de risques d'attaque, de vol et de détournement. Les exemples étrangers sont à cet égard inquiétants et rappellent que le risque de fuite de données n'est jamais nul (...).** »⁵

² Cf. rapport d'information sur l'usage de la biométrie en France et en Europe n°688, établi par MM. François BONHOMME et Jean-Yves LECONTE, sénateurs, 13 juillet 2016.

³ Comme indiqué ci-dessus, un tel traitement impliquerait un changement des finalités du fichier TES (sensibilité politique) et des modifications réglementaires.

⁴ Coût des télécommunications estimé à 3,7 M€ TTC + 440 k€ TTC à l'étranger (source : ANTS).

⁵ Avis Conseil national du numérique fichier TES décembre 2016.

Autrement dit, **même dans l'hypothèse où les obstacles juridiques et techniques seraient levés pour la création d'un tel fichier, il serait probablement d'une utilité faible pour des traitements d'identification** et d'authentification (cas C et D évoqués supra) au vu des mesures contraignantes de sécurité qu'il conviendrait de mettre en place, au vu de sa sensibilité : ligne dédiée, pas de possibilité de traitements de masse, pas d'interrogation directe sur la donnée biométrique⁶.

Pour toutes ces raisons, une architecture reposant sur la création d'un fichier centralisé ne paraît pas judicieuse. Cela a pour conséquence, si une solution biométrique reposant sur une technologie « embarquée » s'avérait finalement retenue, qu'il ne sera pas possible de procéder à un traitement d'identification des assurés sociaux, c'est-à-dire d'écartier toute possibilité que l'empreinte d'un assuré soit référencée plusieurs fois sur des cartes différentes, autrement dit de s'assurer qu'un assuré dispose d'une et une seule carte Vitale⁷.

1.1.2. La technologie embarquée apparaît plus praticable

Le recours à une technologie biométrique embarquée sur le support permettra d'effectuer un traitement d'authentification en évitant le recours à une base de données centralisée. Les données personnelles biométriques des utilisateurs sont donc sécurisées dans la puce figurant sur le support par un mécanisme de chiffrement, donc en l'occurrence sécurisées sur une carte Vitale « biométrique ».

Une telle solution d'authentification devra respecter les normes européennes du règlement eIDAS et être certifiée par l'ANSSI, potentiellement à un niveau équivalent à celui de la CNIe, du fait de la sensibilité des données contenues dans la puce (niveau d'authentification de sécurité dit élevé)⁸.

La lecture de la donnée biométrique pourrait s'effectuer en fonction des technologies retenues (empreintes digitales, reconnaissance faciale) :

- ◆ soit directement à partir d'un capteur d'empreintes digitales intégré à la carte Vitale. La carte à puce intègre alors à la fois une fonction de stockage (de la donnée biométrique de référence) et une fonction de comparaison (comparaison de l'empreinte apposée sur le capteur avec celle présente dans la puce sécurisée) : cette technologie d'authentification biométrique dite « *match-on card* » permet de s'assurer de la concordance entre les empreintes du porteur et les données de la carte.
- ◆ soit à partir du capteur de la caméra intégrée à l'équipement du professionnel de santé. Dans cette hypothèse, plus complexe à mettre en œuvre, une interface est nécessaire entre l'équipement dont dispose le professionnel de santé et la carte à puce, qui n'a plus qu'une fonction de stockage de la donnée biométrique de référence : la fonction de comparaison est portée par une application exécutée par le logiciel du professionnel de santé.

⁶ Par exemple, pour le fichier TES, le seul cas métier prévoyant un accès aux données biométriques de TES est la réquisition judiciaire.

⁷ Alors qu'un tel traitement biométrique aurait permis de simplifier le contrôle prévu à l'article R. 161-33-1 du code de la sécurité sociale, qui dispose que « *lors de la mise à disposition d'une carte Vitale, l'organisme vérifie que le titulaire de la carte n'est possesseur d'aucune autre carte valide sous la même forme* ».

⁸ Depuis 2014, le règlement eIDAS n°910/2014 définit un socle commun pour tous les échanges sécurisés entre les citoyens, les entreprises et les autorités publiques au sein de l'Union européenne. Trois niveaux de sécurité (faible, substantiel et élevé) correspondent à des besoins distincts. La CNIe est de niveau élevé.

1.2. La fréquence d'usage envisagée est également structurante

Une fois la donnée biométrique de l'assuré référencée (sur la puce d'une carte ou dans une base centralisée), la fréquence du contrôle biométrique opéré à partir du support peut être programmée ou paramétrée par le logiciel de lecture de la puce :

- ◆ l'appel à un traitement biométrique peut être systématique à chaque lecture de la puce, c'est-à-dire lors de chaque visite chez un professionnel de santé en ville, à chaque passage à l'officine pour retirer des médicaments, ou en établissement de santé – c'est à dire à chaque fois qu'il est nécessaire de s'assurer de l'existence de droits ;
- ◆ le recours à une vérification biométrique peut être programmé de manière aléatoire, ou à un rythme régulier (par exemple tous les 10 passages), ou calé sur une fréquence calendaire (par exemple une fois tous les trimestres). Il s'agit d'une version moins invasive de la biométrie à l'usage ;
- ◆ le traitement biométrique peut être réduit à une seule occurrence, lors de l'activation de la puce, c'est-à-dire lors de la phase d'enrôlement, à réception de la carte, à la suite d'une première demande ou d'un renouvellement.

Graphique 1 : Schéma de traitement d'authentification



Source : GIE SESAM Vitale.

Plus la fréquence du recours à un contrôle biométrique du porteur d'une carte biométrique est élevée, plus le risque de mésusage ou de fraude au porteur décroît. Ainsi, pour réduire significativement le risque d'usurpation d'identité, c'est-à-dire le prêt d'une carte à un autre assuré, le recours au contrôle biométrique du porteur de la carte doit être généralisé, systématique et obligatoire.

Cette hypothèse d'un recours systématique au contrôle biométrique a été présentée à un large ensemble d'interlocuteurs (syndicats, ordres, personnalités qualifiées) parmi les professionnels et établissements de santé.

Les réponses convergent largement sur les difficultés apportées par le dispositif, des nuances apparaissant entre les professionnels libéraux (cf. 1.2.1), qui utilisent quotidiennement la carte Vitale, et les professionnels exerçant en établissement (cf. 1.2.2), notamment public, qui, eux, ne l'utilisent presque pas et pourraient même s'en passer.

1.2.1. L'appréciation des professionnels de santé libéraux

Les syndicats, ordres et professionnels interrogés (médecins généralistes, infirmiers libéraux, pharmaciens) ne remettent pas en question la nécessité de lutter contre la fraude à l'Assurance maladie et contre le mésusage de la carte Vitale même s'ils rapportent qu'ils ont, dans leur ensemble, été très peu souvent confrontés à de tels cas dans leur exercice.

Annexe VI

L'acceptabilité d'un tel dispositif est faible avec, dans plusieurs cas, une réception hostile à l'idée d'un tel projet. Certains ont indiqué qu'ils s'y opposaient « *catégoriquement* », par exemple la Fédération des Syndicats Pharmaceutiques de France, indiquant que les inspections pouvaient mentionner cette position expressément dans le rapport. Aucun ne s'est montré ouvertement favorable à la mise en place d'un contrôle biométrique de son porteur.

Tous se sont en revanche interrogés sur l'opportunité de la mise en place d'un tel dispositif (qui a été qualifié de « hors sujet » par deux des interlocuteurs de la mission).

Plusieurs arguments sont présentés :

- ◆ la relation entre un patient et un professionnel de santé repose sur la confiance. Or, contrôler l'identité du porteur revient à entamer ce lien de confiance, d'autant plus que la biométrie a un caractère intrusif ;
- ◆ le métier d'un professionnel de santé n'est pas de faire un contrôle de l'identité mais de soigner ou de dispenser des médicaments et des dispositifs médicaux ;
- ◆ la majorité de la clientèle est connue et identifiée de beaucoup de professionnels de santé (malades chroniques, familles soignées depuis des décennies, personnes âgées...) : s'assurer de leur identité à chaque visite paraît, pour ces patients, inutile et incongru ;
- ◆ dans les cabinets médicaux, effectuer un contrôle biométrique ajoute un temps administratif supplémentaire, qui, même s'il est minime, s'additionne au fil de la journée et réduit le temps consacré aux patients et au soin, dans un contexte où l'attention se porte sur l'accroissement du temps médical⁹ ;
- ◆ dans le cas des pharmacies, un tel contrôle occasionnera, *a minima*, une augmentation des files d'attente (voire un engorgement de l'officine en période de pointe). Au pire, il empêcherait la délivrance du médicament à un tiers. Or, d'après certains pharmaciens interrogés, entre 30 % et 50 %¹⁰ des personnes qui se présentent en officine viendraient retirer les médicaments pour le compte d'un tiers ou ayant droit : souvent un membre de la famille, une assistante maternelle, une aide à domicile présente une ordonnance pour le compte d'une personne malade ou étant dans l'incapacité de se déplacer, d'un enfant mineur, du conjoint, d'une personne âgée ou handicapée, résidente en EHPAD, personne sous tutelle ou curatelle.

Dans le cas des interventions au domicile des patients, les infirmiers libéraux s'interrogent sur le sens d'un tel contrôle, réalisé au sein même du domicile du patient, voire de sa faisabilité et, là aussi, de son caractère incongru (sinon « *indécent* »), citant par exemple le cas d'un contrôle biométrique réalisé au petit matin, pour des personnes âgées alitées, d'autant que les patients n'ont pas toujours leur carte Vitale sur eux. Les syndicats sont au mieux réservés : un syndicat infirmier serait favorable à un contrôle biométrique « *à condition que cela ne rajoute pas de contrainte* », et « *seulement si cela ne représente pas un temps supplémentaire* »¹¹. Or un tel système biométrique représenterait à l'évidence une procédure et un temps administratif supplémentaire.

⁹ À cet égard, le retour d'expérience des contrôles biométriques opérés aux frontières, où ils sont en principe obligatoires, montre qu'ils sont rarement réalisés, faute de temps (rapports de l'inspection générale de l'administration).

¹⁰ La mission ne dispose pas d'éléments chiffrés permettant de déterminer la proportion exacte des usagers se présentant en officine pour retirer un médicament pour le compte d'un tiers, toutefois, elle n'a pas de raison de mettre en cause les déclarations des professionnels rencontrés, qui ont tous évoqué une part importante de la clientèle.

¹¹ Propos issus des entretiens.

Annexe VI

Un des interlocuteurs de la mission a constaté une tendance à l'augmentation des flux dégradés, liée au choix des infirmiers libéraux de gagner du temps en regroupant les opérations de facturation des soins aux patients en fin de journée ou en fin de mois – c'est-à-dire en s'assurant de l'ouverture des droits dans ADRI et sans recourir à la carte Vitale des patients. Cette dégradation se fait au prix des sommes forfaitaires – jugées trop modiques – versées en contrepartie de l'atteinte d'un taux d'émission minimal de feuilles de soin électroniques (FSE).

Par ailleurs certains de nos interlocuteurs ont évoqué les difficultés à mettre en place un contrôle au porteur pour la population des enfants mineurs et des personnes majeures protégés.

Encadré 2 : Les mineurs et majeurs protégés

Deux catégories d'assurés sociaux présentent des particularités rendant particulièrement difficile l'usage de la biométrie :

- les mineurs relevant de l'aide sociale à l'enfance ;
- les majeurs protégés (sous curatelle et surtout sous tutelle).

En effet, s'agissant de leur santé, ces personnes dépendent d'un tiers, qui peut être une personne morale représentée par des personnes physiques variant au cours du temps (exemple : un mineur placé en établissement, et dont la carte vitale sera détenue successivement par plusieurs éducateurs).

La difficulté de la dispensation de médicaments en officine pour ces populations vient de la multiplicité et la variabilité des personnes susceptibles de chercher des médicaments pour leur compte. Ainsi, la délégation de carte Vitale apparaît particulièrement complexe à mettre en œuvre pour ces personnes.

Source : Mission.

Enfin, les effets d'un tel contrôle, en cas de non-reconnaissance biométrique du porteur, interrogent l'ensemble des professionnels de santé :

- ◆ sur le risque induit pour leur sécurité avec un probable accroissement des incivilités et des agressions. Ce point, majeur, a été relevé par la totalité des intervenants ;
- ◆ sur le risque d'augmentation des flux de facturation dégradés et donc du temps administratif de gestion consacré à l'envoi de feuilles papier ;
- ◆ sur le glissement que cela signifierait symboliquement, passant d'une fonction de soins à une fonction de contrôle administratif : les professionnels de santé refusent de façon catégorique et unanimement de procéder à un contrôle de l'identité « approfondi », en demandant au patient de justifier de son identité, en particulier si le contrôle biométrique est négatif ;
- ◆ de manière générale, les professionnels rencontrés se sont montrés interrogatifs sur les conséquences pratiques sur son exercice que devrait tirer un professionnel de santé à l'occasion de la découverte d'une usurpation d'identité. Il serait alors mis face à une double contrainte déontologique, qui ne pourrait se résoudre que par un acte gratuit de sa part :
 - l'obligation de soin (le serment d'Hippocrate des médecins ou chirurgiens dentistes, ou le serment de Galien des pharmaciens), cette obligation existant pour l'ensemble des professionnels de santé ;
 - l'interdiction de participer à une opération frauduleuse¹² – la découverte de l'usurpation d'identité lui permettant d'avoir pleinement conscience qu'une facturation à l'assurance maladie serait frauduleuse.

¹² CSP, articles R. 4127-221 pour les chirurgiens-dentistes, R. 4312-81 pour les infirmiers, R. 4321-77 pour les masseurs kinésithérapeutes, R. 4127-29 pour les médecins, R. 4322-43 pour les podologues et R. 4127-337 pour les

Annexe VI

Enfin, tous les professionnels souhaitent un dispositif s'intégrant aux projets en cours de déploiement de l'INS et de l'application carte Vitale et qui aille dans le sens de la simplification du parcours des patients et de leur équipement (logiciel et matériel) de cabinet (pas de lecteur biométrique supplémentaire) tout en maintenant la garantie de paiement.

1.2.2. En établissement, une préoccupation plus liée à l'identitovigilance qu'à la fraude

En établissement, s'assurer de l'identité des patients est une nécessité sanitaire dans une optique d'identitovigilance¹³. Toutefois les patients peuvent refuser de présenter une pièce d'identité : si le code de la sécurité sociale prévoit bien la possibilité pour un établissement de santé de contrôler l'identité d'un patient par la production d'un titre d'identité avec photographie, il est muet sur la conduite à tenir en cas de refus du patient. En d'autres termes, si le patient refuse de produire le document d'identité requis, aucun texte n'interdit à l'établissement de délivrer le soin, ce qui est en pratique systématiquement le cas.

L'authentification de l'identité est généralement demandée à l'admission lorsque les soins sont programmés (séjour ou ambulatoire). Lorsque le patient arrive en situation d'urgence vitale, la priorité est au soin et le patient peut justifier de son identité postérieurement à sa prise en charge. Il est d'ailleurs pris en charge sans condition en cas de soins urgents et vitaux, ce qui rend en pratique inutile l'usurpation d'identité.

Au centre hospitalier Avicenne, la consultation systématique du téléservice CDRI pour obtenir les droits à jour du patient rend la consultation des droits en puce de la carte Vitale inutile : seul le NIR présent sur la carte est utilisé et sert à la consultation des téléservices CDR et CDRI. L'ajout d'un contrôle biométrique viendrait alourdir la procédure d'admission, dans un tel contexte : en effet, dans l'hypothèse d'un gabarit biométrique stocké sur la carte, il faudrait à nouveau insérer la carte dans un lecteur pour effectuer le traitement de comparaison.

De plus, les admissions peuvent se faire, pour une part non négligeable, en dehors de la présence physique du patient. Ainsi, à la demande de la mission, le service des admissions de l'hôpital Avicenne a recensé, durant une semaine, les personnes se présentant au guichet (cf. tableau ci-dessous). C'est au total plus d'un patient sur cinq qui n'est pas physiquement présent lors de son admission.

Tableau 2 : Qualité des personnes se présentant au guichet des admissions entre le 6 et le 7 février 2022 au centre hospitalier d'Avicenne, Seine Saint Denis

-	6 février	7 février	8 février	9 février	10 février	Total
Patient	35	33	24	12	13	119
Famille	6	2	2	9	4	23
Service	3	0	2	2	2	9
Ambulance	0	0	0	0	2	2

Source : service des admissions, hôpital Avicenne.

Enfin, l'usage de la biométrie viendrait à contre-courant du mouvement de dématérialisation et de préadmission et d'admission à distance engagé par les établissements, qui investissent fortement dans ces solutions, afin de réduire les coûts mais aussi fluidifier les parcours patients.

sages-femmes. Curieusement des dispositions équivalentes semblent ne pas exister pour les pharmaciens, pour lesquels l'article R. 4235-9 se limite à énoncer : « dans l'intérêt du public, le pharmacien doit veiller à ne pas compromettre le bon fonctionnement des institutions et régimes de protection sociale. Il se conforme, dans l'exercice de son activité professionnelle, aux règles qui régissent ces institutions et régimes ».

¹³ L'identitovigilance est l'ensemble des mesures mises en œuvre pour fiabiliser l'identification de l'usager afin de sécuriser ses données de santé, à toutes les étapes de sa prise en charge, cf. encadré *infra*.

Annexe VI

Outre les éléments présentés *supra*, les personnels des établissements rencontrés en charge de la gestion des admissions et de la facturation considèrent la mise en place d'un tel contrôle inutile :

- l'effet d'un tel contrôle augmentera le risque d'incivilités, notamment dans les services d'urgence en cas d'urgence non vitale et au service des admissions ;
- pour une fédération, la mise en place d'un contrôle biométrique présente un risque de renoncement aux soins qu'elle considère « *important* ».

S'agissant des personnels soignants, l'information selon laquelle un patient est ou non assuré social, ou ressortissant ou non du dispositif AME n'est pas pertinente : unanimement, les soignants hospitaliers ont affirmé qu'ils avaient l'obligation éthique de soigner toutes les personnes se présentant à eux. Si une fraude à l'identité devait être détectée, le soin serait tout de même assuré. En d'autres termes, le sujet de la fraude à l'identité n'est perçu que comme une difficulté en termes d'identitovigilance (qui vise la qualité et la sécurité des soins) et non comme une difficulté financière, car le soignant – et son établissement – est dans l'obligation d'effectuer le soin.

1.2.3. La fréquence d'un contrôle biométrique pourrait être réservée aux situations les plus critiques en termes de risques de fraude

Il ressort de ces éléments que la fréquence du traitement biométrique peut difficilement être paramétrée de manière systématique, c'est-à-dire à chaque interaction avec un professionnel de santé.

Il pourrait être décidé, dans un souci de simplicité, de désactiver systématiquement le contrôle biométrique de la carte en officine, en raison du risque sanitaire encouru par une personne malade (perte de chance) faute de pouvoir délivrer un médicament à un tiers, et a contrario de l'activer systématiquement en cas de délivrance de médicament coûteux (au-delà d'un certain montant) ou pour certaines spécialités pharmaceutiques (stupéfiants...).

Il pourrait aussi être envisagé de désactiver ce traitement biométrique, à supposer que cela soit techniquement faisable, par exemple :

- ◆ hors les cas de première visite, pour les visites réalisées chez son médecin traitant ;
- ◆ hors les situations de première prise en charge, pour les soins réalisés sur de longues périodes (kinésithérapie, soins d'hygiène par les infirmiers libéraux...) ;
- ◆ hors les situations d'admission ou de première prise en charge, en établissement ou au domicile du patient.

Il serait également intéressant d'étudier les modalités (techniques ou juridiques) d'activation d'un tel contrôle, au-delà d'un certain montant d'actes de soins auprès du professionnel de santé ou au-delà d'un certain montant de médicaments délivrés en officine, voire de manière aléatoire.

Evidemment, plus le nombre de situations où il est renoncé de recourir à un contrôle biométrique est élevé, plus l'intérêt présenté par une solution biométrique diminue.

1.3. Le recueil de la donnée biométrique à l'enrôlement lors d'une demande d'une carte Vitale

1.3.1. La procédure actuelle de remise de la carte Vitale est simple mais apparaît robuste

La commande d'une carte Vitale (première demande ou renouvellement) est une démarche qui peut être effectuée en ligne de manière dématérialisée à partir du compte Ameli, pour les assurés en disposant, ou par courrier : elle ne nécessite pas de se rendre au guichet d'une caisse primaire.

Toutefois, à la CPAM de Seine-Saint-Denis, entre 4 % et 5 % des usagers contactent la caisse ou se rendent au guichet pour un motif en lien avec la carte Vitale, le plus souvent une commande.

La procédure de remise d'une carte Vitale n'est pas sécurisée par une délivrance en main propre à son titulaire : la carte, une fois émise, est transmise par courrier simple à l'assuré à l'adresse de son lieu de résidence tel qu'il est connu de son organisme d'assurance maladie. Ce faible formalisme ne semble pas poser de difficultés : il n'a pas été signalé à la mission le cas de vols (massifs) de cartes Vitale à leur réception (par les CPAM interrogées comme par le GIE SESAM Vitale). S'ils existent, ces cas sont anecdotiques.

La sécurisation de cette phase, par une remise en main propre, ou même un envoi par pli recommandé, paraît donc peu pertinente en termes de lutte contre la fraude.

1.3.2. La mise en place d'un contrôle biométrique nécessiterait de recueillir les données biométriques des assurés sociaux

En l'absence d'un tiers pour vérifier l'identité de la personne à l'enregistrement du gabarit de référence de la solution biométrique, l'authenticité de ce gabarit n'est pas garantie (i.e. le gabarit enregistré peut être celui d'une personne différente de l'assuré).

L'hypothèse de la création d'une carte Vitale biométrique pose donc la question des conditions matérielles du recueil de la donnée biométrique :

- ◆ soit en « face à face », par exemple dans les caisses primaires, auprès des professionnels en ville voire des établissements de santé ;
- ◆ soit à distance, à l'instar de l'expérimentation (en cours) pour l'application « carte Vitale » lors de son installation : l'utilisateur est guidé pour réaliser un selfie vidéo et comparer l'image obtenue avec celle de sa carte d'identité. Le caractère asynchrone de cet enrôlement est à la fois un avantage (organisation simplifiée, possibilité d'y procéder à toute heure) et un inconvénient (pas d'enrôlement en temps réel, l'assuré pouvant attendre durant une durée significative avant d'être enrôlé dans le système).

Pour l'ANSSI, le caractère irrévocable du facteur inhérent fait de la phase d'enregistrement une phase « *très critique* » qui « *doit être protégée en conséquence* » : elle recommande de « *favoriser une rencontre en présence lors de l'enregistrement d'un facteur inhérent* » pour vérifier l'identité¹⁴.

¹⁴ ANSSI « recommandations sur la sécurisation des systèmes de Contrôle d'accès physique et de vidéoprotection », 4/3/2020.

Annexe VI

C'est par exemple le cas pour les demandes de titres régaliens sécurisés : le recueil des empreintes digitales est effectué par les services d'état civil des mairies pour la carte nationale d'identité et le passeport. Ce n'est pas le cas des photographies d'identité, qui constituent un maillon faible de la chaîne sécuritaire dans la mesure où elles ne sont pas prises dans des conditions de sécurité équivalentes à celles des empreintes digitales.

Ainsi, tous les systèmes d'enrôlement par l'image sont risqués en raison du risque de manipulation de ces images. Les pirates ou les fraudeurs ont recours à des « *deep fakes* » (images très réalistes), portent des masques, utilisent des vidéos, découpent des photos, ou encore ont recours à du maquillage pour leurrer la reconnaissance faciale.

Les autorités publiques sont confrontées depuis une dizaine d'années au développement des techniques de *morphing*¹⁵ (détectée pour la première fois dans un aéroport allemand en 2013 sur un passeport britannique), ce qui conduit certains Etats (Allemagne) à réinternaliser la prise de photographie, lors de l'instruction des demandes de titres d'identité¹⁶.

D'après l'ANTS, les outils de *morphing* sont facilement accessibles et extrêmement efficaces (difficiles à détecter) depuis 2016, ce qui renforce la nécessité de procéder à un enrôlement du demandeur en face à face.

1.3.3. Le coût en ETP supplémentaires du seul enrôlement en face à face s'élèverait à plusieurs centaines de millions d'euros chaque année

En raison des options retenues par le gouvernement (maximisation du temps soignant et minimisation du temps administratif), la mission a écarté l'hypothèse d'un enrôlement effectué par des professionnels de santé.

De même, en raison des difficultés rencontrées pour l'établissement des titres d'identité, la mission a écarté l'hypothèse d'un alignement des modalités d'établissement de la carte Vitale sur celles des titres sécurisés, qui s'appuient sur 4 100 dispositifs de recueil / remise en mairie¹⁷.

La mission a donc examiné trois méthodes estimatives :

- ◆ en s'inspirant des travaux effectués par l'IGAS en 2004 ;
- ◆ en reprenant les travaux de la CNAM ;
- ◆ en effectuant ses estimations sur la base des données fournies par la CPAM de Seine-Saint-Denis.

¹⁵ La photographie fournie est une création artificielle reprenant à la fois les traits du porteur légitime du titre (dans cet hypothèse complice de son usurpation d'identité) et du porteur réel, illégitime du titre : l'algorithme de reconnaissance faciale identifiera les deux personnes comme étant celle représentée dans la photographie traitée par *morphing*.

¹⁶ La Bulgarie, le Portugal, la Suède et la République tchèque privilégient l'enrôlement de l'image en face-à-face pour leurs titres d'identité.

¹⁷ Auxquels s'ajoutent environ 400 dispositifs de recueil en postes consulaires. Source : ANTS.

1.3.3.1. L'actualisation de l'estimation effectuée dans le cadre de la mission de l'IGAS de 2004 aboutirait à un coût annuel de 240 M€

Un rapport de l'IGAS de 2004¹⁸ estimait le surcoût de l'apposition d'une photographie d'identité sur la carte Vitale avec un enrôlement en face à face à l'assurance maladie à 160 M€ pour 50 millions de cartes : le surcoût de l'opération de face à face (dont la durée était estimée à 5 minutes) était évalué à un surcoût de 2,50 € par carte émise¹⁹.

Si l'on retient l'hypothèse que le dépôt d'une photo d'identité en 2004 prend le même temps de recueil qu'une donnée biométrique en 2022 (apposition du pouce ou de l'index, photo pour reconnaissance faciale), on peut évaluer le coût d'un enrôlement en face à face, sur la base d'une hypothèse constante, rapporté au parc actuel de 58 millions de cartes et corrigé de l'érosion monétaire²⁰, à un montant annuel de 241 M€ en euros 2022 (hors coût d'un renouvellement du parc tous les cinq ans).

1.3.3.2. L'estimation de la CNAM s'établit aux alentours de 300 M€

Le coût de la captation des données biométriques en caisse primaire, en face à face est estimé par l'Assurance maladie à 300 millions d'euros (temps total par assuré 15 minutes multiplié par 58 millions de porteurs de cartes pour un coût horaire de 21 euros²¹), auquel s'ajoute le coût de la formation des agents à la vérification des pièces d'identité et le coût matériel de l'équipement (non chiffrés par l'Assurance maladie).

Par ailleurs la CNAM estime à 129 M€ le surcoût annuel associé aux FSE dégradées et aux feuilles de soins papier.

1.3.3.3. La mission estime que le coût en ETP d'un enrôlement biométrique des assurés sociaux serait de l'ordre de 535 M€, tout en étant très dépendant de la fréquence de renouvellement du stock de cartes Vitale biométriques

Dans les deux hypothèses précédentes, le temps passé en « face-à face » est évalué à hauteur de 5 minutes par assuré (pour l'IGAS en 2004), et de 15 minutes (pour la CNAM). Il n'est pas tenu compte des coûts de coordination, de la durée d'instruction du dossier de demande dans son ensemble.

À l'issue de ses investigations et en échangeant avec la CPAM de la Seine Saint Denis, la mission estime qu'un délai de 20 minutes pour le dépôt d'une demande de carte vitale biométrique, couplée à un enrôlement, paraît plus raisonnable.

La mission a établi ses hypothèses de travail en se basant sur un comportement inchangé des assurés, c'est-à-dire en ne tenant pas compte des effets du prochain déploiement de l'ApCV (cf. annexe relative à l'application carte Vitale), et de l'effet potentiellement dissuasif de la mise en place d'un contrôle biométrique sur la carte physique.

¹⁸ Rapport IGAS n° 2004-066 « Les risques de fraude à l'assurance maladie », établi par Carine Chevrier-Fatome, François Mercereau, Pascal Penaud et Dr Sylvain Picard, juin 2004.

¹⁹ Évalué par la mission à partir des données de l'assurance maladie et de la DSS.

²⁰ Cf. calculatrice INSEE en ligne.

²¹ Coût horaire moyen estimé par l'Assurance maladie.

Annexe VI

D'un point de vue théorique, pour renouveler le parc en une année le nombre d'agents supplémentaires total en caisses locales est estimé à 12 919 ETP, soit un coût de masse salariale chargée de 535 M€ au total (cf. tableau ci-dessous)²².

En pratique, le renouvellement du parc de cartes, au vu de son étendue (57,9 millions) devra être étalé sur plusieurs années. La mission retient deux durées : 5 années, ce qui correspond à la durée de vie d'une carte biométrique avec capteur et 10 années, dans l'hypothèse d'une carte sans capteur, mais dont il faut renouveler à l'issue de ce délai le gabarit²³. Les estimations ne tiennent pas compte du renouvellement intermédiaire des cartes perdues ou volées.

Actuellement, près de 4 millions de nouvelles cartes sont produites²⁴ chaque année. Le renouvellement complet du parc sous 5 ou 10 années représenterait une augmentation sensible de la production de cartes pour le GIE-SESAM Vitale, qui devraient gérer la production de respectivement 11,6 ou 5,8 millions de cartes annuelles.

Dans l'hypothèse où le parc serait totalement renouvelé en cinq années, un renouvellement en face à face de ces cartes nécessiterait donc la mobilisation par l'assurance maladie de 2 584 ETP annuels supplémentaires à l'échelle nationale (pour 11,6 millions de cartes²⁵) pour un coût salarial (toutes charges comprises) estimé à 107 M€, ce coût ne tenant pas compte des besoins de renouvellement intermédiaire du parc nouvellement constitué.

Dans l'hypothèse où le parc serait totalement renouvelé en dix années, un renouvellement en face à face de ces cartes nécessiterait donc la mobilisation par l'assurance maladie de 1 292 ETP annuels supplémentaires à l'échelle nationale (pour 5,8 millions de cartes²⁶) pour un coût salarial (toutes charges comprises) estimé à 53 M€, ce coût ne tenant pas compte des besoins de renouvellement intermédiaire du parc nouvellement constitué.

Le coût supplémentaire total en ETP de la création d'un parc de carte Vitale biométrique sera étalé dans le temps dans la limite de la fréquence de rotation du parc biométrique.

Tableau 3 : Évaluation du nombre d'ETP nécessaires en caisse primaire pour l'enrôlement biométriques de l'ensemble des cartes Vitales valides à date

Hypothèse en fonction du délai de remplacement retenu pour les cartes	1 an	5 ans	10 ans
Nombre cartes à produire par an (*)	57 900 000	11 580 000	5 790 000
Temps RDV/carte (pré-accueil, accueil, enregistrement) (en minutes)	20	20	20
Temps RDV total (en heures)	19 300 000	3 860 000	1 930 000
Besoin ETP RDV	12 452	2 490	1 245
Sollicitations/réclamations (+ 5%)	2 895 000	579 000	289 500
Besoin ETP sollicitations/réclamations	467	93	47
Besoin ETP total	12 919	2 584	1 292
Coût annuel total chargé en ETP, en € (**)	535 357 564	107 071 513	53 535 756

²² Coût total « brut », qui doit donc être divisé en fonction de la durée choisie pour renouveler le parc.

²³ Effet de vieillissement du vivant, entraînant un taux de rejet injustifié plus important et une dégradation des performances du système (augmentation des anomalies...).

²⁴ Carte Vitale - production 2022 : 3,9 millions de cartes (2021 : 3,9 millions ; 2020 : 3,6 millions ; 2019 : 4 millions).

²⁵ On prend pour hypothèse une diminution de 25 % du nombre de demandes de cartes Vitale physiques du fait de la montée en charge de l'application e-cV.

²⁶ On prend pour hypothèse une diminution de 25 % du nombre de demandes de cartes Vitale physiques du fait de la montée en charge de l'application e-cV.

Annexe VI

Source : Mission sur la base des hypothèses de la CPAM Seine Saint Denis.

(*) Hypothèses de comportement des usagers inchangé.

(**) Coût annuel chargé par ETP estimé à partir des données UCANSS et <https://www.urssaf.fr/portail/home/utile-et-pratique/estimeur-de-cotisations.html?ut=estimeurs>

1.3.4. L'enrôlement biométrique pourrait voir son coût réduit s'il se faisait à distance

Il ressort donc de ces considérations que l'enrôlement biométrique :

- ◆ doit être réalisé en « face-à-face » pour sécuriser l'enregistrement de données biométriques : toutefois, un recours au face à face reviendrait à mobiliser les agents des caisses primaires d'assurance maladie, dans des proportions élevées²⁷ ou les professionnels de santé, qui considèrent dans leur ensemble qu'ils n'en ont ni le temps, ni la compétence ;
- ◆ peut être réalisé de manière dégradée si l'on ne souhaite pas sécuriser cette étape : l'enrôlement (la prise de gabarit de référence) peut être réalisé par l'assuré seul ou à distance, si l'on considère qu'il n'est pas dans son intérêt qu'il enregistre une donnée biométrique (photo, empreinte digitale) autre que la sienne :
 - pour la technologie de l'empreinte digitale, la capture d'empreintes serait rendue possible à domicile en fournissant avec la carte un kit d'enregistrement²⁸ (dont le prix de vente est de l'ordre de 4€ à 5 € par lecteur, à ajouter au prix de vente de la carte),
 - pour la technologie de la reconnaissance faciale, il serait également possible de demander à l'utilisateur de fournir une photographie numérisée à l'appui de sa demande de carte.

Dans ces deux derniers cas, toutefois, la fraude à l'identité n'est pas déjouée et l'authenticité de la donnée biométrique ne pourrait être garantie²⁹.

Toutefois, même dans cette dernière hypothèse, une partie de la population en situation d'illectronisme devra être accompagnée pour pouvoir réaliser cette opération. D'après la CPAM de Seine-Saint-Denis, les demandes en lien avec la carte Vitale (essentiellement commande et suivi) représentent environ 4 % à 5 % des motifs de contact (physique et téléphonique) des usagers. Il est probable que la mise en place d'une technologie biométrique, même dans l'hypothèse d'un enrôlement à distance, aura un effet inflationniste, difficile à quantifier.

²⁷ Ce qui ne serait pas cohérent avec la stratégie de gestion des relations avec les usagers, qui vise à réduire l'accueil au guichet et à dématérialiser les démarches administratives.

²⁸ Ce dispositif d'enrôlement à LED et piles est un kit « jetable » qui permet d'enregistrer l'empreinte lorsqu'elle est présentée la première fois sur le capteur.

²⁹ Il serait toutefois possible de sécuriser une étape a minima en ajoutant une opération supplémentaire après la réalisation d'un gabarit sans face à face : ce gabarit pourrait être activé a posteriori par l'envoi sous pli séparé d'un code d'activation du gabarit (même modèle que le système de délivrance des cartes bancaires, où le code de la carte est envoyé sous pli séparé) – ce qui n'empêcherait pas les cas de détournement avec complicité de l'assuré.

Une alternative consisterait à recourir à la même solution que celle utilisée pour l'application carte Vitale, c'est-à-dire à une source biométrique déjà authentifiée (la photo de CNIe) pour déjouer le maximum de cas de fraude, ce qui implique l'usage de la reconnaissance faciale comme technologie biométrique afin de pouvoir générer, à distance une photo pour le gabarit de référence (selfie), et ce qui implique l'utilisation d'un smartphone. Pour la population n'en disposant pas ou n'y parvenant pas (soit entre 10 % et 20% des usagers)³⁰, un passage au guichet serait donc toujours nécessaire. Le coût de l'enrôlement par reconnaissance faciale sur l'application carte Vitale a été estimée par la GIE SESAM Vitale pour l'application carte Vitale à un euro par an et par utilisateur (sans négociation et échanges supplémentaires avec d'éventuels fournisseurs logiciels). Toutefois, dans ce cas, la technique utilisée ne pourrait être que la reconnaissance faciale.

1.4. L'empreinte digitale et la reconnaissance faciale sont, en France, mieux acceptées que la reconnaissance de l'iris

La mission s'est intéressée aux principales techniques déployées à large échelle (cf. 1.4.1). Parmi celles-ci, l'empreinte digitale et la reconnaissance faciale apparaissent comme les techniques suscitant le moins de réticence (cf. 1.4.2). La fiabilité et la sécurité apparaissent néanmoins comme des facteurs à prendre en compte (cf. 1.4.3).

1.4.1. Certaines modalités biométriques sont désormais utilisées à grande échelle

Parmi l'ensemble des modalités biométriques, trois technologies sont disponibles sur le marché via des kits de développement logiciels (SDK), ce qui facilite leur implémentation à grande échelle :

- ◆ les empreintes digitales ;
- ◆ la reconnaissance faciale ;
- ◆ l'iris (en Inde).

Le principe de fonctionnement, les avantages/inconvénients de ces différentes modalités ont été présentées dans annexe relative au recours à la technologie biométrique .

1.4.2. Des modalités biométriques bénéficient d'une bonne acceptation dans la population française

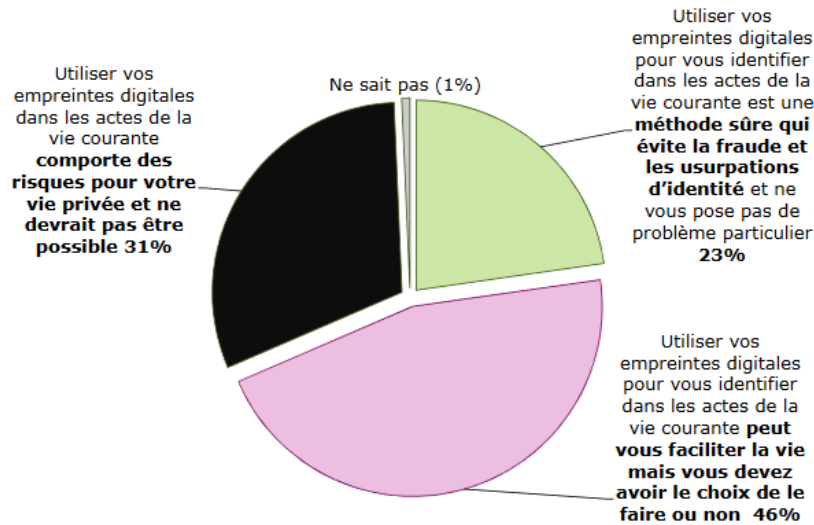
Le taux d'acceptation des usagers varie selon leur familiarité avec la technologie, leur perception de l'intrusion, de l'effort nécessaire (temps et geste requis de l'utilisateur) et de l'exactitude du système. En 2013, plus de deux tiers des français étaient prêts à utiliser leurs empreintes digitales pour s'identifier dans la vie courante³¹ (cf. graphique 2).

³⁰ 87% des français ont un smartphone d'après le baromètre du numérique 2002. <https://www.vie-publique.fr/en-bref/288030-barometre-du-numerique-les-chiffres-cles-2022>; 77% d'après l'INSEE (janvier 2022).

³¹ CREDOC, Enquête « Conditions de vie et Aspirations », début 2013.

Annexe VI

Graphique 2 : Réponses à une enquête de 2013 du CREDOC, « les empreintes digitales pourraient être utilisées pour vous identifier dans la vie courante : pour accéder au travail, payer dans les magasins, etc. Quelle opinion se rapproche le plus de la vôtre ? », en %



Source : CREDOC, Enquête « Conditions de vie et Aspirations », début 2013.

Ce taux d'acceptation a progressé. D'après l'enquête réalisée par le Défenseur des droits en octobre 2022, « près des trois quarts des Français voient dans le développement des technologies biométriques et de leurs usages une bonne chose et y associent principalement des traits d'image positifs, les considérant pour plus des deux tiers d'entre deux comme pratiques, efficaces, ou encore fiables. »³²

En avril 2021, selon un sondage réalisé en France par GetApp, parmi les répondants reconnaissant avoir soumis au moins une donnée biométrique (33 % des personnes interrogées), passeport mis à part et dans un contexte autre que médical (c'est-à-dire à l'exclusion du sang, de la salive, etc.), 66 % déclarent avoir effectué cette démarche pour l'authentification biométrique sur mobile et 34 % pour réaliser un paiement ou une opération en ligne³³. A la question « données de santé mise à part, quelles données biométriques personnelles accepteriez-vous de partager avec des entreprises privées ? (plusieurs réponses possibles) », 38 % des répondants répondent : « aucune », 42% l'empreinte digitale, 31 % le visage, 27 % la voix et 20 % l'iris.

En février 2022, dans une enquête réalisée par l'entreprise Capterra, le partage des empreintes digitales était la modalité biométrique la mieux acceptée³⁴.

³² Enquête du Défenseur des droits réalisée en octobre 2022 : « Perception du développement des technologies biométriques en France : entre manque d'information et demande d'encadrement » ;

³³ GetApp Biometrics and Facial recognition survey, 2021 - Pour recueillir ces données, GetApp a interrogé un total de 1 009 répondants sur le territoire français. Le nombre de répondants peut varier d'une question à l'autre, selon la logique du sondage. Celui-ci a été mené du 14 au 19 avril 2021. Les répondants devaient être âgés de plus de 18 ans et résider en France. <https://www.getapp.fr/blog/1992/58-pourcent-francais-estiment-naivoir-jamais-partage-donnees-biometriques>

³⁴ Source : enquête Capterra, février 2022 - Nombre de répondants : 716. Réponse à la question : parmi les types suivants de données biométriques personnelles, lesquelles seriez-vous à l'aise de partager avec des entreprises privées, à l'exclusion de prestataires de soins de santé ? (plusieurs réponses possibles) je ne suis pas à l'aise avec le partage des informations citées : 47%, empreintes digitales 28%, voix 23%, géométrie de la main 16%, iris 15%, vaisseaux sanguins 6%, tests ADN 3%.

Annexe VI

Du fait de son caractère ressenti comme intrusif et du caractère contraignant de son acquisition³⁵, la modalité biométrique de l'iris paraît devoir être écartée des scénarios praticables. Développer une solution en recourant à l'iris exposerait l'assurance maladie à des refus d'enrôlement, et à des comportements d'évitement vers des supports jugés moins intrusifs (application carte Vitale, attestation des droits papier).

Les deux premières technologies (empreintes digitales, reconnaissance faciale) sont mieux acceptées des usagers. S'agissant de la reconnaissance faciale, un praticien a rapporté à la mission le refus d'environ 1 % à 2 % de ses patients de se faire prendre en photo pour figurer dans le fichier informatisé des patients tenu par son établissement de soins. Certains professionnels de santé évoquent aussi dans leur patientèle le cas des femmes voilées ou portant un foulard ou les patients portant des masques, susceptibles de rendre un tel contrôle plus difficile à mettre en œuvre.

1.4.3. Les deux modalités à forte acceptabilité, empreinte digitale et reconnaissance faciale, présentent des performances éprouvées sous réserve d'un compromis à trouver entre expérience utilisateur et niveau de sécurité

Les rapports de test du le *National Institute of Standards and Technology* (NIST) consultables en ligne, comme les industriels, font état d'excellentes performances pour la reconnaissance faciale. De même le GIE SESAM Vitale fait état dans son étude d'excellentes performances relativement à l'authentification biométrique (ex : ~1/100 000 pour les faux positifs¹, 4/500 pour les faux négatifs). Toutefois le fonctionnement en condition réelle de la reconnaissance faciale semble entraîner une dégradation rapide des performances comme semble en attester l'absence de pérennisation de certaines expérimentations (Roland Garros, carnaval de Nice, Aéroport de Paris cité par l'un de nos interlocuteurs).

D'un autre côté, le GIE SESAME Vitale, dans son étude sur la biométrie, relève la diversité des lecteurs d'empreintes digitales, dont le niveau de fiabilité peut être très variable selon le type de capteur (lecteur à capteur optique, capacitif ou ultrason) et les caractéristiques de l'appareil, ce qui rend compliqué le déploiement d'un tel dispositif à grande échelle et diminue la performance générale de la solution : « *La construction du gabarit est basée sur la capture de l'empreinte, qui elle-même dépend du type de technologie de capteur utilisée. Mettre en place un algorithme unique fonctionnant avec tous les types de capteurs est donc délicat* ».

Nos interlocuteurs sont partagés s'agissant des performances algorithmiques respectives des empreintes digitales et de la reconnaissance faciale. Pour certains experts, les algorithmes de reconnaissance faciale enregistrent des taux de faux négatifs moyens (entre 3 % et 5%) bien supérieurs à ceux qui reconnaissent les empreintes digitales (moins de 1 %).

Toutefois, ces performances se dégradent au fil du temps. Ainsi, si le taux d'erreur est inférieur à 1% pour les empreintes digitales des adultes lors de la remise d'un titre sécurisé, un mois après avoir déposé la demande et enregistré le gabarit, il atteint 25 % lors de la demande de renouvellement du titre, soit 10 années après le dernier enrôlement.

S'agissant d'un dispositif qui a vocation à couvrir quasiment l'ensemble de la population, il semble toutefois préférable de privilégier un scénario biométrique embarquant la technologie la plus éprouvée et dont les performances semblent moins discutables (sous réserve d'un compromis sécurité / expérience utilisateur acceptable, cf. analyse supra) et la plus connue des assurés, en l'occurrence celle des empreintes digitales.

³⁵ À la date de la mission. Les dernières versions des capteurs sont moins intrusives.

2. La mission a plus particulièrement évalué deux solutions embarquées utilisant les empreintes digitales ou la reconnaissance faciale

2.1. La reconnaissance des empreintes digitales, outre un surcoût significatif par rapport à la situation actuelle, risque de faire apparaître un nombre important de faux négatifs

Comme indiqué supra, l'architecture retenue devrait être décentralisée. Si la donnée biométrique retenue est l'empreinte digitale, les minuties des doigts (ou, plus précisément, leur gabarit) seraient stockés sur la carte Vitale (cf. 2.1.1). Déployée à cette échelle, cette technique biométrique ferait très probablement apparaître un grand nombre (dans l'absolu) de faux négatifs (cf. 2.1.2). Par ailleurs, les coûts liés à l'usage de ce type de cartes Vitale, en dehors des coûts d'enrôlement décrits supra, seraient très sensiblement supérieurs à ceux de la carte Vitale actuelle (cf. 2.1.3).

2.1.1. Le gabarit des minuties des doigts est stocké sur la carte Vitale

L'empreinte présente sur la puce de la carte Vitale sera utilisée comme gabarit de référence : son authenticité sera garantie (ou non) en fonction de la procédure retenue pour l'enrôlement (face à face ou non). Il est par ailleurs techniquement possible de stocker deux empreintes (voire trois, d'après les fabricants) sur la carte de type « match on card », par exemple si la première empreinte ne marche pas.

À l'usage, lorsqu'une authentification biométrique sera demandée, le lecteur de la carte Vitale procédera à la comparaison entre l'empreinte déposée sur le capteur et l'empreinte référencée dans la puce.

Les performances des algorithmes permettant de générer le gabarit et d'effectuer la comparaison du gabarit à l'empreinte sont mesurées lors de l'attribution de la conformité à la norme *Minutiae Interoperability Exchange* (Minex) de niveau III, établie par le *National Institute of Standards and Technology* (NIST) américain³⁶ : les taux de fausses acceptations et de fausses non correspondances (FNMR) des algorithmes certifiés sont bas³⁷.

³⁶ <https://www.nist.gov/itl/iad/image-group/minutiae-interoperability-exchange-minex-iii>

³⁷ Toutefois le taux de fausses non-correspondances ne correspond qu'à une partie des rejets : il n'intègre pas les rejets à la suite de la non-acquisition de l'empreinte (ce qu'intègre le taux de faux rejets, FRR non publié dans les rapports NIST disponibles en ligne).

2.1.2. La large diffusion de la solution risque de mettre en évidence un nombre important d'échecs à l'usage

Une des principales limites d'une telle solution est liée aux conditions de leur utilisation en condition réelle : il existe un écart entre les performances mesurées par les fabricants et celles effectivement constatées dans différents environnements. Pour les empreintes digitales, le taux de faux négatif peut augmenter sensiblement du fait des conditions extérieures de température (sensibilité du doigt au froid) et d'humidité (insensibilité du capteur à un doigt humide, ou à un doigt qui pèle...). Le taux de rejet d'utilisateurs légitimes est estimé à hauteur de 1 % (3 % en 2016 par la CNIL), soit potentiellement environ 600 000 titulaires de cartes Vitale³⁸. Le GIE SESAM Vitale estime le taux d'échec en condition d'usage entre 2 % et 5 % (soit, appliqué aux titulaires de cartes Vitale, entre 1 158 000 et 2 895 000 assurés)³⁹. En dehors de l'usage carte Vitale, deux banques commercialisent en France pour leurs clients des cartes bancaires biométriques de type « match on card » (voir *infra*). Pour le GIE cartes bancaires, il s'agit à ce stade d'un marché de niche en termes de diffusion de la solution. Les fabricants des cartes confirment qu'à peine quelques dizaines de cartes sont produites par jour. Il n'a pas été communiqué à la mission par les industriels le taux de rejet en conditions d'utilisation réelles, ni de retour d'expérience des usagers, ce qui tend à accréditer le caractère novateur de la technologie devrait inciter à la prudence.

2.1.3. La solution biométrique engendrerait des coûts de production entre deux et 10 fois supérieurs à la solution actuelle

Si les gabarits biométriques sont stockés dans la carte, la lecture de l'empreinte peut s'effectuer de deux manières.

Dans un premier sous scénario (« match on card »), la lecture est effectuée par la carte Vitale elle-même qui dispose d'un lecteur intégré.

Une telle solution nécessite toutefois le remplacement d'une partie du parc de lecteurs de cartes Vitale, sans qu'il soit possible de déterminer leur nombre à ce stade. En effet, l'apposition de l'empreinte sur le lecteur présent sur la carte nécessite que cette dernière soit insérée de manière horizontale, et que le lecteur soit découvert. Or, certaines configurations de lecteurs ne remplissent pas ces conditions (insertion verticale).

Le coût de production d'une carte biométrique avec un lecteur intégré est évalué entre 10 € et 20 € selon nos interlocuteurs (comparé aux 2,07 € pour la carte actuelle). En prenant une hypothèse basse de 12 € (incluant les coûts de gestion à hauteur de 2€ par carte), le coût de renouvellement du parc complet de cartes Vitale en 2023⁴⁰ s'élèverait donc à 695 M€. Cette hypothèse ne tient pas compte toutefois du changement de comportement des assurés qui préféreront disposer uniquement d'une application carte Vitale, ce qui entraînera une diminution de la demande de carte physique, et donc du coût de la mesure. La diminution des demandes de cartes physiques risque d'être d'autant plus importante que l'enrôlement nécessiterait un déplacement physique au guichet de la CPAM⁴¹.

Pour rappel, le coût total de production de la carte actuelle est de 2,63 €. Le coût total d'une carte biométrique serait 4 à 5 fois plus élevé.

³⁸ Estimation à partir du parc de cartes Vitale actuel : 57,5 M de cartes.

³⁹ Source : Q01-T01-01-Rencontre_IGAS-IGF_carte_Vitale_biométrique_20221208_v2.pdf

⁴⁰ Parc de 57,9 millions de cartes Vitale en 2021.

⁴¹ Sauf à privilégier un enrôlement sans contrôler l'identité de l'assuré : dans ce cas il faut rajouter à la carte le coût du kit pour s'enrôler.

Annexe VI

Dans l'hypothèse où il faudrait renouveler 50 % des lecteurs de carte Vitale (parc de 410 000 lecteurs standards selon GIE SESAM Vitale), le coût serait de :

- ◆ 205 000 lecteurs « standards » de carte Vitale au coût unitaire de 30 € (estimation GIE SESAM Vitale), soit 6,15 M€ ;
- ◆ par ailleurs, les appareils disponibles en pharmacie d'officine⁴², au nombre 50 000 ou en établissement de santé⁴³, plus complexes car permettant aussi bien la lecture que l'écriture (mise à jour des droits) représenteraient un coût unitaire plus important mais que la mission n'a pas pu évaluer.

Au coût du matériel s'ajoutent nécessairement des coûts de développement logiciels (non estimés) et des coûts de licence d'utilisation concernant les interfaces logicielles des éditeurs de solutions (professionnels de santé, établissements), si le logiciel de la puce est amené à échanger des informations avec le logiciel du professionnel de santé (par exemple en cas de conditionnement du contrôle biométrique au montant des actes de soins pratiqués, ou en fonction du montant total des médicaments délivrés, ou encore si on souhaite « inhiber » la fonction biométrique lorsque le professionnel de santé est un pharmacien pour permettre à des tiers de se voir délivrer les médicaments du patient). Dans ce cas, il n'est pas possible de se prononcer sur le rythme de mise à jour des éditeurs de logiciel des professionnels de santé, si une telle mise à jour s'avérait nécessaire, ni sur le choix des professionnels d'effectuer ou non la mise à jour (souvent payante).

Dans un second sous scénario, le lecteur d'empreintes digitales est un appareil distinct de la carte.

Le coût de production d'une carte biométrique, sans capteur d'empreinte digitale est évalué entre 5 € et 10 €, d'après les interlocuteurs de la mission. Une carte biométrique sans capteur serait donc *a minima* deux fois plus coûteuse que la carte Vitale actuelle.

Dans cette hypothèse, le capteur d'empreinte digitale ne se trouvant pas sur la carte, un lecteur d'empreintes digitales devra s'ajouter au matériel installé chez le professionnel de santé / en établissement de santé :

- ◆ pour les professionnels de santé : 410 000 capteurs mono-doigt à 100 € (coût évalué entre 100 € et 500 € selon les modèles) soit 41 M€ ;
- ◆ la question des appareils d'écriture sur la carte Vitale, qui sera plus complexe – et plus protégée – si elle contient le gabarit de l'empreinte digitale, demeure (cas des pharmacies d'officine et établissements de santé).

Au coût des lecteurs s'ajoutent potentiellement des coûts de développement logiciels (non estimés) et des coûts de licence d'utilisation concernant les interfaces logicielles des éditeurs de solutions (professionnels de santé, établissements), si le logiciel de la puce est amené à échanger des informations avec le logiciel du professionnel de santé (par exemple en cas de conditionnement du contrôle biométrique au montant des actes de soins pratiqués, ou en fonction du montant total des médicaments délivrés). Dans ce cas, il n'est pas possible de se prononcer sur le rythme de mise à jour des éditeurs de logiciel des professionnels de santé, si une telle mise à jour s'avérait nécessaire, ni sur le choix des professionnels d'effectuer ou non la mise à jour (souvent payante).

⁴² 100 000 lecteurs en pharmacie d'après SESAM Vitale.

⁴³ D'après la DREES, on dénombre près de 3 000 établissements de santé en 2022. Toutefois, en fonction de leur taille, ceux-ci peuvent détenir entre quelques et plusieurs dizaines de terminaux de lecture/écriture de cartes Vitale.

2.2. La reconnaissance faciale est probablement moins onéreuse mais n'offre pas de garanties en termes de faux négatifs

2.2.1. Une photographie de haute résolution ou un gabarit des traits du visage sont stockés en carte

La carte Vitale porterait soit un gabarit d'éléments biométriques liés au visage, soit plus simplement une photographie d'une résolution suffisante pour mettre en œuvre la reconnaissance faciale. La procédure retenue pour l'enrôlement influera fortement sur le caractère probant de cette photographie.

La solution nécessite la présence d'une caméra frontale sur l'ensemble des postes des professionnels de santé / officines de pharmacie / établissements de santé (service des admissions), soit a minima 410 000 caméras chez les professionnels de santé, 50 000 en officine, sans compter ceux déployés en établissement de santé.

À l'usage, lorsqu'une authentification biométrique sera demandée, les images issues de la caméra frontale du professionnel de santé ou de l'établissement d'une part et d'autre part celle issue de la carte Vitale (ou le gabarit en résultant) seront confrontées.

2.2.2. La reconnaissance faciale engendre aussi un nombre important de faux négatifs pour un usage massif, tout en étant très sensible aux conditions d'acquisition du gabarit

Les principales limites de cette solution est la dégradation du taux de faux rejets négatifs du fait du port de masque, des conditions de luminosité, de la position du visage, port de lunettes, de foulard, etc. Le taux de rejet à l'enrôlement d'utilisateurs légitimes est estimé à hauteur de 1% par le GIE SESAM Vitale (pour l'application ApCV), soit potentiellement environ 600 000 titulaires de cartes Vitale (dans l'hypothèse où tous téléchargent l'application).

Par ailleurs, si l'utilisateur fournit une photographie, quand bien même elle serait contrôlée par les services de l'assurance maladie, le recours à des techniques de *morphing* (permettant à plusieurs personnes d'être reconnues par le dispositif biométrique comme ayant une seule et même identité) ne peuvent être exclus : la qualité de l'enrôlement est donc essentielle.

2.2.3. Les surcoûts liés à cette technique apparaissent plus limités que la technique biométrique

Une caméra devra s'ajouter au matériel installé chez le professionnel de santé ou en établissement de santé :

- ◆ 410 000 caméras avec reconnaissance faciale (professionnels de santé) (coût évalué à *a minima* 150 € par caméra) soit au moins 60 M€ ;
- ◆ 50 000 caméras en officine : 15 M€ ;
- ◆ Montant en établissement de santé : fonction des besoins des établissements.

Au coût des lecteurs s'ajoutent les coûts de développement logiciels (non estimés) et des coûts de licence d'utilisation concernant les interfaces logicielles des éditeurs de solutions (professionnels de santé, établissements), si le logiciel de la puce est amené à échanger des informations avec le logiciel du professionnel de santé (par exemple en cas de conditionnement du contrôle biométrique au montant des actes de soins pratiqués, ou en fonction du montant total des médicaments délivrés). Dans ce cas, il n'est pas possible de se prononcer sur le rythme de mise à jour des éditeurs de logiciel des professionnels de santé, si une telle mise à jour s'avérait nécessaire, ni sur le choix des professionnels d'effectuer ou non la mise à jour (souvent payante).

2.3. Les coûts liés au déploiement d'une carte Vitale biométrique sont de l'ordre de 1 milliard d'euros

2.3.1. La mission n'a pas pu évaluer les coûts de développement

La reconnaissance faciale comme la reconnaissance digitale sont des solutions de biométrie dont l'usage s'est répandu ces dernières années : les développeurs de solutions / industriels commercialisent des bibliothèques de SDK (Software Development Kit)⁴⁴ évitant ainsi un développement complet et diminuant ainsi les coûts et les délais de mise en œuvre associés. Toutefois la mission n'a pas pu évaluer les coûts de développement de telles solutions.

2.3.2. Au total, la solution biométrique apparaît très onéreuse

Actuellement, les cartes Vitale émises n'ont pas de date de fin de validité : le parc de cartes Vitale est technologiquement hétérogène, avec des cartes très anciennes et d'autres plus récentes. La part importante du parc de cartes Vitale 1, les plus anciennes, démontre la robustesse du support physique des cartes actuellement en usage.

Le déploiement d'une carte Vitale biométrique devra s'effectuer sur plusieurs années, car il n'est pas envisageable de renouveler 57,9 millions de cartes en une, ou même deux années.

La durée de vie d'une carte biométrique avec capteur a été évaluée à environ 5 années au maximum par les industriels, notamment du fait du caractère moins durable de ses composants. Pour les cartes avec capteur, la durée de vie de la carte est inversement proportionnelle au nombre de lectures. Les opérateurs bancaires prévoient le renouvellement des cartes bancaires biométriques tous les trois ans⁴⁵.

Dans l'hypothèse d'un renouvellement tous les cinq ans, 11 580 000 de cartes devraient donc être fabriquées chaque année (non compris les cas d'usure anticipée, de perte ou de vol de carte).

Le coût annuel de maintien en condition opérationnelle d'une carte biométrique est estimé au minima à 246 M€ (empreinte digitale sur 5 ans) ou à 94 M€ (reconnaissance faciale sur 10 ans), hors les coûts d'investissement au démarrage (plus faibles pour les empreintes digitales que pour la reconnaissance faciale) et l'ensemble des coûts associés ci-dessous, pour lesquels la mission n'a pu disposer de données (cf. tableau page ci-après).

⁴⁴ Kit de développement logiciel.

⁴⁵ Ce qui illustre bien que si l'on retient une durée de vie de cinq années pour les cartes Vitale biométriques, un certain nombre de cartes devra être renouvelée avant leur date d'échéance théorique, sans que l'on puisse en estimer la proportion, faute de retour d'expérience.

Annexe VI

Pour rappel, le coût de gestion et de production annuel du renouvellement du parc de cartes Vitale actuel par le GIE SESAM Vitale est de l'ordre d'environ 17 M€⁴⁶.

Encadré 3 : Coût de gestion et de production du renouvellement actuel de la carte Vitale (2021)

Le coût global actuel de gestion d'une carte vitale est estimé à 4,33€ et se décompose comme suit :

Le coût de production d'une carte Vitale est de 2,63 € et se décompose comme suit :

Coûts de production 2,07 €	Numérisation de la photo	0,38 €	} Coûts de production actuel 2,63 €
	Fabrication de la carte vierge	0,52 €	
	Personnalisation	0,62 €	
	Envoi de carte Vitale à l'assuré	0,54 €	
Coûts de gestion 0,56 €	Gestion par le GIE SESAM-Vitale	0,56 €	

Et le coût de gestion par les agents en caisse par carte Vitale émise estimé à environ 1,7€.

Source : CNAM.

Dans l'estimation effectuée par la mission, plusieurs hypothèses ont été formulées :

- ◆ le comportement des assurés est inchangé (même nombre de demande de cartes) ;
- ◆ les cas de renouvellements anticipés de la carte du fait d'une perte ou d'un vol ne sont pas pris en compte ;
- ◆ des hypothèses basses de coût de production sont retenues de 5 € pour une carte biométrique sans capteur et de 10€ pour une carte avec capteur, sans toutefois à ce stade pouvoir tenir compte des économies réalisées sur la production d'une carte à grande échelle ;
- ◆ les coûts associés à la majoration du nombre de FSE dégradées ou feuilles de soins papier, évalués à 129 M€ par an par l'Assurance maladie (estimation CNAM de 5 % de FSE sécurisées en moins), n'ont pas été intégrés.

Par ailleurs, les mesures de sécurité du dispositif (cf. règlement eIDAS) devront être maximales en raison du risque de compromission des données, ce qui induit probablement un surcoût, qu'il est difficile de chiffrer à ce stade.

Quelle que soit la fréquence du renouvellement retenue, le déploiement de la biométrie nécessite une augmentation sensible des capacités de production des industriels, qui produisent annuellement près de 4 millions de cartes Vitale. La production des cartes bancaires biométriques est actuellement très faible (quelques dizaines par jour, à l'échelle nationale).

⁴⁶ Coût de gestion global de 4,33 € par carte Vitale pour un total de 4 millions de cartes produites annuellement.

Annexe VI

Enfin, il convient d'attirer l'attention sur l'accroissement de l'exposition à deux risques :

- la production d'un plus grand nombre de cartes accroît la dépendance technologique aux industriels, fournisseurs de normes et composants, dont une partie sont fabriqués à l'étranger (exposition au risque de pénurie) ;
- le choix de la technologie biométrique accroît le risque d'obsolescence technologique du composant sécuritaire de la puce (chiffrement) et de créer une dépendance technologique avec l'industriel retenu, dans l'hypothèse d'un gabarit propriétaire⁴⁷.

Enfin la technologie biométrique augmente le coût de production en termes de développement durable (cartes en polycarbonate). A ce stade les industriels ne se prononcent pas sur la possibilité de produire de telles cartes à partir de matériaux recyclés.

⁴⁷ Par exemple la première génération de cartes Vitale est devenue assez facilement piratable, ce qui emporte peu de conséquence, en l'absence de donnée biométrique contenue sur ce support.

Annexe VI

Tableau 4 : Estimation non exhaustive du coût annuel de production et d'utilisation d'une carte Vitale biométrique selon deux modalités biométriques en euros (*)

-	Coût total de la solution sur 5 ans ou 10 ans pour la totalité du parc	Empreintes digitales (ED) avec capteur intégré / Hypothèse de renouvellement tous les 5 ans	Reconnaissance faciale (RF) avec gabarit dans la puce / Hypothèse de renouvellement tous les 10 ans (*)
CONCEPTION / DEVELOPPEMENT / EQUIPEMENT			
Équipement en lecteurs des professionnels de santé : 410 000 (fonction lecture) à 30 € (ED) ou 150 € (caméra)	12 300 000 (ED) 61 500 000 (RF)	12 300 000	61 500 000
<i>Sont à déterminer dans le cadre d'une étude de faisabilité, les coûts relatifs à :</i> - Équipement des caisses primaires en lecteurs - Développements logiciels assurance maladie (implémentation traitement biométrique dans SI cV) - Développements éditeurs logiciels des professionnels libéraux et établissements de santé - Équipement en lecteurs des pharmacies (50 000 avec fonction écriture) et établissements (lecture et/ou écriture) - Formation des personnels en CPAM à l'enrôlement des données biométriques - Développement du système d'information de gestion des anomalies/ signalements par la CNAM (traitement des rejets)			
FONCTIONNEMENT/MAINTIEN EN CONDITION OPERATIONNELLE			
Coût des ETP pour l'enrôlement biométriques en face à face en CPAM (20 minutes par rendez-vous) et pour les sollicitations/réclamations	535 357 564	107 071 513	53 535 756
Coût de fabrication de la carte (10 € pour ED, 5 € pour RF)	579 000 000 (ED) 289 500 000 (RF)	115 800 000	28 950 000
Coût de gestion de la carte par le GIE SESAM Vitale (2 € par carte)	115 800 000	23 160 000	11 580 000
<i>Sont à déterminer dans le cadre d'une étude de faisabilité, les coûts relatifs à :</i> - Coût MCO de la maintenance des matériels / logiciels (***) - Procédure alerte en cas d'échec : gestion des anomalies/ signalements par la CNAM (coût ETP)			
Sous total Fonctionnement	1 230 157 564 (ED) 940 657 564(RF)	246 031 513	94 065 756
Coût total (développement, déploiement, fonctionnement)	1 242 457 564 (scénario 'empreintes digitales' sur 5 ans) 965 257 564 (scénario 'reconnaissance faciale' sur 10 ans)		

Source : Mission d'après CNAM, CPAM 93, GIE SESAM Vitale, ANTS, IN Groupe.

(*) Il est nécessaire de renouveler régulièrement le gabarit pour éviter dégradation du taux de rejet.

(**) L'usage de la carte Vitale biométrique entraînerait 5 % de FSE sécurisées en moins dues à des problèmes de rapprochement d'identité avec l'usage de la biométrie (notamment en cas de faux négatif) et donc un nombre plus important de factures générées en mode dégradés et/ou de FSP, et donc avec moins de contrôle, ce qui est l'opposé de l'objectif visé.

(***) Par exemple, bien que le dispositif envisagé soit différent, la maintenance des matériels des titres sécurisés (« stations lourdes ») représente entre 3500 et 6100 interventions terrain par an, pour un coût estimé de maintenance à 2,9 M€ par an. Source : ANTS.

Annexe VI

Schématiquement, la solution avec capteur d'empreintes digitales intégré est plus coûteuse, de l'ordre de 1,2 M€ au total (cf. graphique 3), que celle avec l'implémentation de la reconnaissance faciale, de l'ordre de 965 M€ (cf. graphique 4), mais probablement plus simple à mettre en œuvre, en termes de développements logiciels et matériels.

Graphique 3 : Coût du scénario d'une carte Vitale biométrique avec capteur d'empreintes digitales et un renouvellement du parc sur 5 années



Source : Mission.

Graphique 4 : Coût du scénario d'une carte Vitale biométrique avec reconnaissance faciale et un renouvellement du parc sur 10 années



Source : Mission.

À noter que le déploiement progressif de ces deux scénarios entraîne également un surcoût lié au maintien en condition de fonctionnement du parc actuel de cartes non biométriques et de ses équipements logiciels et matériels, non intégré à l'estimation.

2.4. Le recours à la biométrie ne peut s'envisager sans mettre en place de solution alternative, en cas notamment de faux négatif

Comme il n'est pas possible de garantir le fonctionnement de la solution biométrique pour 100 % des usagers, quelle qu'en soit la modalité retenue, il faut prévoir des solutions alternatives (cf. 2.4.1). Une surveillance des cas atypiques devrait dans ce cas être effectuée par l'assurance maladie (cf. 2.4.2). À défaut de système alternatif simple, la question du risque – et de la personne le supportant – en cas de faux négatif devrait être traitée (cf. 2.4.3).

2.4.1. Un système alternatif doit permettre l'accès aux droits garantis par l'assurance maladie

Un système alternatif à la carte Vitale biométrique doit permettre, en toute hypothèse, aux assurés sociaux d'exercer effectivement leurs droits. En effet :

- ◆ il n'existe pas dans la législation actuelle d'obligation pour un assuré de détenir une carte Vitale, et encore moins d'obligation d'utilisation d'une carte Vitale. Une simple attestation de droits suffit. S'agissant du régime général, cette attestation de droits est téléchargeable depuis le compte Ameli de l'assuré, sans mesure de sécurisation particulière. Le nombre de téléchargements n'est pas limité, et son émission sous un format PDF ne prévoit pas un nombre limité d'utilisations. **À droit constant, un assuré social peut ne pas détenir de carte Vitale, ou ne pas l'utiliser, et faire usage d'attestations papier. Cet usage met en échec l'authentification permise par une carte Vitale biométrique ;**
- ◆ il n'existe pas plus, pour le professionnel ou l'établissement de santé, d'obligation d'utilisation d'une carte Vitale pour vérifier les droits ouverts à la prise en charge des frais de santé ou établir la facturation des actes de soins. Les mesures promouvant son usage sont incitatives et conventionnelles. Au surplus, il est possible de vérifier l'ouverture des droits d'un assuré par d'autres moyens (téléservices ADRI/CDRI, compte Ameli Pro) sans carte Vitale. Au total, si l'assuré social n'est pas tenu d'utiliser la carte Vitale, **le professionnel de santé n'est, à droit constant, pas tenu non plus de l'accepter ;**
- ◆ dans l'hypothèse où il ne serait pas donné la possibilité à un usager de s'opposer au recueil des données biométriques dans la puce de la carte Vitale, il n'est pas impossible que le nombre de demandes de cartes Vitale diminue, un petit pourcentage d'usagers préférant garder le contrôle de leurs données biométriques et préférant faire valoir leurs droits à partir d'une simple attestation papier ;
- ◆ plusieurs cas d'usage ont été identifiés par la mission, qui nécessiteraient la déconnexion du contrôle biométrique car l'usage de la carte Vitale d'autrui (cas notamment de la **pharmacie**), voire l'absence d'usage de la carte Vitale (pour des raisons techniques, cas des **analyses biologiques** ou de la **télé médecine** ; pour des raisons de confidentialité cas de la **santé sexuelle des mineurs**) est aujourd'hui considérée comme légitime. **Sauf à poser des difficultés majeures au système de santé, ces cas d'usage pour autrui ou de non usage de la carte Vitale devraient être pris en compte dans un cadre biométrique, venant limiter l'efficacité du dispositif ;**

Annexe VI

- ◆ les performances des algorithmes pouvant varier sensiblement en fonction des caractéristiques vivantes de la personne (âge, handicap, croissance ou vieillissement, blessures...), de la construction de l'algorithme (risque de biais pour certaines catégories de la population), de la performance du capteur (capteur défaillant, dysfonctionnel...), de l'environnement (conditions de température, humidité, luminosité...), **un système alternatif peut s'avérer nécessaire, pour traiter les cas de faux négatifs** (rejets à tort par le système biométrique d'une personne ayant pourtant des droits), voire écarter le contrôle biométrique de manière systématique, par exemple pour les personnes en situation de handicap, majeurs et mineurs protégés, etc.

Pour ce faire, il est possible de proposer des solutions alternatives :

- ◆ en mettant en œuvre parallèlement une seconde technique biométrique. Les coûts associés seraient alors cumulatifs, et il faudrait s'assurer qu'il n'existe pas – ou très peu – de doubles faux négatifs (personnes exclues simultanément par les deux techniques biométriques) ;
- ◆ en mettant en place d'un code secret sur la carte Vitale (code PIN à 4 ou 6 chiffres, comme pour l'application carte Vitale⁴⁸): toutefois le code secret, à l'instar de celui mis en place pour les cartes bancaires, peut être oublié, perdu, volé ou récupéré de manière frauduleuse. Il nécessite le déploiement de procédures de gestion sécurisées (renvoi de code, mécanisme de mise en opposition...), dont le coût viendrait s'ajouter à celui de la mise en place de la biométrie, qui n'a pas été évalué par la mission. En outre, cette solution ne résout pas, à droit constant, le problème de non équipement en carte Vitale.

2.4.2. La nécessité de mettre en place une procédure d'alerte de l'assurance maladie pour traiter les cas de rejets (positifs ou négatifs)

En cas de non-reconnaissance par la technologie biométrique du porteur, l'ensemble des professionnels de santé considère qu'il n'est pas de leur compétence de procéder à un contrôle de l'identité « approfondi » du porteur de la carte Vitale et font valoir, outre leur obligation déontologie de soins, quelle que soit l'identité du patient, le risque induit pour leur propre sécurité.

Aussi, si le contrôle biométrique échoue, une notification de rejet devra pouvoir être générée auprès de services de l'Assurance maladie, à charge pour la caisse primaire de procéder à des investigations plus poussées, s'agissant du motif de rejet.

De plus, en l'absence de présentation d'une carte Vitale par un patient, une multiplication des flux de facturation en mode dégradé (c'est-à-dire un comportement « atypique ») devrait pouvoir être détectée, ce qui implique probablement, à terme, des moyens en personnel supplémentaires pour ne pas engorger les services de la caisse primaire, en charge de la validation des flux de facturation dégradés.

2.4.3. La question de la personne sur laquelle le risque repose en cas de faux négatif (rejet injustifié) doit être tranchée

En l'absence de système alternatif, la question du paiement du professionnel de santé, lorsque l'assuré dispose de droits lui permettant de ne pas avancer les frais, se pose dans le cas des faux négatifs qui sont, par hypothèse, impossible à distinguer des négatifs réels.

⁴⁸ Ce code PIN pourrait ou non être activé (cf. exemple de la carte de santé en Allemagne).

Annexe VI

Ainsi, afin de ne pas s'exposer à un rejet de la prise en charge de l'acte par l'assurance maladie, le professionnel de santé peut être tenté de demander au patient d'effectuer un paiement, charge à lui de se faire rembourser ultérieurement par son organisme d'assurance maladie. Or, la loi prévoit que le patient, dans certains cas, est dispensé de l'avance de frais. Le faux négatif expose donc soit le patient pour qui les droits établis par la loi ne seraient pas respectés, soit le professionnel de santé qui aura effectué un acte sans être rémunéré.

Toute mise en place d'un système biométrique devrait clarifier qui, de l'assurance maladie (ce qui reviendrait à amoindrir considérablement la fonction de lutte contre la fraude du système biométrique), du professionnel de santé ou du patient supporte *in fine* le risque financier lorsque le système biométrique conclut à un défaut d'authentification.

2.5. En conclusion, la mise en place d'une carte Vitale biométrique serait onéreuse tout en ne présentant, en raison des spécificités de l'assurance maladie, que peu de garanties

L'étude de ces différents scénarios montre qu'aucune solution ne répond parfaitement à l'enjeu de développer un système qui, à l'usage, serait fonctionnel partout, systématiquement et obligatoire :

- ◆ il n'est pas possible de garantir le fonctionnement de la solution biométrique pour 100 % des usagers, quelle qu'en soit la modalité : il faut donc prévoir des solutions alternatives, qui en renchérisse sensiblement le coût ;
- ◆ il existe de nombreuses voies de contournement : l'effet dissuasif tiré de l'image « sécuritaire » de cette technologie sera d'autant moins pérenne pour les fraudeurs potentiels que les prétextes / raisons de la contourner sont nombreuses et recevables ;
- ◆ le déploiement d'une solution biométrique, étalée dans le temps, sera particulièrement complexe à mettre en place (enrôlement en caisse primaire, équipement des professionnels et établissement de santé, communication auprès des professionnels de santé et des patients...) ;
- ◆ le coût d'une telle solution sera important ne serait-ce que pour renouveler, à intervalle régulier (tous les cinq à dix ans), le gabarit biométrique en tenant compte de la durée de vie et de la fragilité des composants embarquées sur le support (entre 3 et 5 ans pour une carte avec lecteur d'empreintes digitales intégré). Ainsi, le coût annuel d'une carte Vitale avec biométrie embarquée est estimé entre 115 et 250 M€ selon que l'on retient un coût de carte à 5 € ou 10 € (comparé aux 7,9 M€ pour la carte actuelle) ;
- ◆ le surcoût en personnel lié à la mise en place d'une procédure d'enrôlement en face à face dans les CPAM, estimé à 373 M€ annuels (coût du personnel uniquement) ;
- ◆ il convient d'ajouter, le cas échéant, le coût supplémentaire des lecteurs / caméras (400 M€ pour des lecteurs d'empreintes, 75 M€ pour des caméras à reconnaissance faciale, hors coût du matériel en établissement de santé).

Au total, le coût annuel d'une solution biométrique peut être estimé entre 1,9 et 2,3 Md€, hors coûts de développement et de mise à jour des logiciels des éditeurs de solution de cabinet ou en établissement et des logiciels de l'Assurance maladie, à comportement des assurés inchangé et hors renouvellements anticipés.

De surcroît, la facturation en flux dégradé par les professionnels de santé et le recours par les usagers aux attestations de droit papier, qui resteront en circulation sans comporter de sécurisation biométrique, constitueront toujours une voie de contournement.

3. Une alternative aux scénarios biométriques : le support de la CNIE et du titre de séjour

A l'occasion des entretiens, plusieurs interlocuteurs de la mission ont estimé le support carte Vitale dépassé dans un contexte d'essor des technologies dématérialisées, dressant la perspective à long terme d'une quasi-généralisation de l'application carte Vitale. Il ressort des entretiens l'intérêt à moyen terme de disposer d'un support physique alternatif, permettant à chacun d'exercer ses droits en matière d'assurance maladie, répondant aux besoins des usagers en matière de lutte contre la fraude (usurpation d'identité), d'identitovigilance et de simplification administrative. Certains d'entre eux ont spontanément évoqué l'idée de faire converger en un support unique la carte Vitale et la carte nationale d'identité.

Il s'agit ici de rappeler les trois fonctions assurées par la carte Vitale, et les rapprocher de celles qui pourraient être tenues par une pièce d'identité (carte nationale d'identité ou titre de séjour) :

- ◆ la carte Vitale porte le NIR, qui est l'identifiant d'une personne au sein du système de sécurité sociale français. La mission propose donc d'insérer le NIR dans la CNIE ou un titre de séjour (cf. 3.5) ;
- ◆ la carte Vitale porte les droits d'assurance maladie des affiliés. Cette fonction, développée à la fin des années 1990, était indispensable à une époque où les télécommunications et systèmes d'information ne permettaient pas les accès aux téléservices qui prévalent de nos jours. Le sujet de l'accès, par le professionnel ou établissement de santé, aux droits en temps réel du patient est donc essentiel (cf. 3.6) ;
- ◆ enfin, la carte Vitale permet aujourd'hui la signature de feuilles de soins électroniques. Cette fonctionnalité, qui permet de substantielles économies et sécurise la facturation de l'assurance maladie, doit bien entendu être maintenue (cf. 3.7).

En effet, considérant les difficultés de mise en œuvre et les coûts totaux de développement et de déploiement des scénarios biométriques, la mission a considéré ce scénario alternatif répond à la fois aux enjeux de sécurisation (lutte contre la fraude, sécurité sanitaire des patients) et de simplification pour les usagers et les professionnels de santé.

Ce scénario alternatif repose sur deux constats :

- ◆ la carte nationale d'identité et les titres de séjour sont largement diffusés dans la population française (cf. 3.3) ;
- ◆ il permet de cumuler les avantages en termes de lutte contre la fraude, de commodité d'usage et d'identitovigilance (cf. 3.1). Il permet en outre de simplifier la gestion des droits des enfants de moins de 16 ans (cf. 3.2).

À l'étranger, les systèmes et solutions mises en place étant sensiblement différents de ceux retenus au niveau national, à l'exception du Portugal. Il convient toutefois d'observer que d'autres pays utilisent un document national d'identité pour s'identifier dans leur système de santé (3.4).

Ce scénario, qui a été accueilli favorablement par les professionnels et établissements de santé rencontrés par la mission (cf. 3.9), s'insérerait dans le calendrier de déploiement de la CNIE (cf. 3.8).

3.1. L'utilisation de la carte nationale d'identité en substitution de la carte Vitale permet d'additionner les gains dans les domaines de la lutte contre la fraude et de l'identitovigilance

Si on le compare au scénario biométrique décrit *supra*, le scénario alternatif reposant sur les pièces d'identité régaliennes, notamment la CNIe, consiste à remplacer le facteur d'authentification biométrique qui est un facteur inhérent à l'individu par un facteur de possession (carte d'identité, titre de séjour). Il remplit la même finalité de lutter contre la fraude ou le mésusage de la carte Vitale :

- ◆ la photographie sur la carte nationale d'identité est récente et de bonne qualité, ce qui mettra fin à la pratique du prêt de carte Vitale « entre amis » (sauf pour les jumeaux) ;
- ◆ la procédure de délivrance et de renouvellement sera sécurisée en face à face ;
- ◆ en outre elle sera rangée ou stockée de manière plus sécurisée (par exemple dans les EHPAD, évitant ainsi la surfacturation par les professionnels de santé).

Du point de vue de la facilité d'usage, il sera toujours possible de prêter sa carte nationale d'identité pour aller chercher un médicament à la pharmacie, mais à un tiers de confiance, ce qui compliquera les retraits de médicaments sur fausse ordonnance par un tiers. La question des paramétrages complexes en fonction du cas d'usage posée par la technique biométrique est donc ici sans objet.

À ces objectifs de lutte contre la fraude s'ajoute un objectif de santé publique en matière d'identitovigilance. En effet, la carte nationale d'identité est un document probant dans les procédures de qualification de l'identifiant national de santé, et la production d'un document présentant une photographie récente et de bonne qualité est mis en avant par les soignants rencontrés par la mission et en charge de cette thématique comme un élément majeur de progrès.

Encadré 4 : L'identitovigilance

L'identitovigilance est l'ensemble des mesures mises en œuvre pour fiabiliser l'identification de l'utilisateur afin de sécuriser ses données de santé, à toutes les étapes de sa prise en charge. Si le contrôle de l'identité est une étape commune à des processus de lutte contre la fraude, le but poursuivi est ici de s'assurer de l'identité du patient afin de sécuriser sa prise en charge par le système de soins. Il s'agit ainsi d'un élément clé de qualité et de sécurité des soins.

Pour ce faire, l'article L. 1470 2 dispose que « l'utilisation des services numériques en santé requiert [une] identification électronique de leurs utilisateurs » reposant « sur un moyen, matériel ou immatériel, qui garantit un niveau adapté de sécurité et de protection des données à caractère personnel traitées ». La loi renvoie à un référentiel, établi par arrêté :

- arrêté du 24 décembre 2019 (JORF du 28 décembre 2019) approuvant la version 1.0 du référentiel national d'identitovigilance ;
- arrêté du 27 mai 2021 (JORF du 8 juin 2021) approuvant les modifications du référentiel et présentant la version 2.0 du référentiel national d'identitovigilance.

Dans sa dernière version⁴⁹, le référentiel national d'identitovigilance comportait cinq volets :

un volet de présentation (volet 0) ;

- un volet commun à l'ensemble des professionnels et modes d'exercice (volet 1) ;
- un volet applicable aux établissements de santé (volet 2) ;

⁴⁹ Les arrêtés d'approbation prévoient que le document annexé soit consulté sur le site de l'Agence du numérique en santé. La dernière version à jour a été consultée sous le lien suivant : <https://esante.gouv.fr/produits-services/referentiel-ins>

Annexe VI

- un volet applicable aux structures non hospitalières⁵⁰ (volet 3) ;
- un volet applicable aux professionnels libéraux (volet 4).

Afin de sécuriser l'identité du patient⁵¹, « *il est indispensable de s'assurer, a minima lors du premier contact physique de l'usager dans une structure, que les justificatifs d'identité présentés correspondent bien à la personne prise en charge* ». Par ailleurs, « *lors de venues ultérieures, ce contrôle de cohérence systématique entre l'identité réelle et celle enregistrée peut ne pas se justifier si l'usager est connu de l'acteur de santé* ».

Les dispositifs à haut niveau de confiance acceptés sont⁵² :

- pour tous les usagers, les dispositifs d'identification électroniques apportant un niveau de garantie substantiel – l'application carte Vitale devant assurer ce niveau de garantie – ou élevé au sens du règlement eDAS⁵³ ;
- pour les usagers français, la carte nationale d'identité et le passeport⁵⁴. Pour les mineurs ou des usagers majeurs qui n'en disposent pas, le livret de famille ou un extrait d'acte de naissance sont acceptés. Toutefois, le représentant légal, (parent, tuteur ou administrateur *ad hoc* pour les majeurs protégés), doit alors justifier de sa propre identité ;
- pour les usagers étrangers, le passeport ou le titre de séjour ;
- pour les ressortissants de l'Union européenne, suisses, liechtensteinois, norvégiens, islandais, vaticans, monégasques, saint marinais et andorrans, la carte nationale d'identité est également acceptée.

Les autres documents d'identité doivent être rejetés.

Source : Mission.

À cet égard, un rapide comparatif des dispositifs mis en place dans d'autres pays européens permet de constater que la présentation de la carte d'identité lors d'une visite chez le médecin est la règle pour certains d'entre eux (Portugal, Suède, Belgique, Monaco, à plus long terme le Danemark), qu'elle soit ou non le support des droits sociaux.

Le scénario proposé simplifie également la situation des enfants de moins de 16 ans.

3.2. L'adoption de la solution « NIR sur CNi » permettrait de simplifier la situation des enfants mineurs, source de difficultés rapportés par l'ensemble de nos interlocuteurs

Actuellement, un enfant de moins de 16 ans est généralement rattaché en qualité d'ayant droit à la carte Vitale d'un des deux parents qui en assurent la charge.

Il peut également être rattaché à la carte Vitale des deux parents. Ce double rattachement génère souvent des difficultés.

⁵⁰ Établissements sociaux et médico-sociaux, structure libérale d'exercice coordonné de plus de 10 professionnels, dispositifs d'appui à la coordination des parcours.

⁵¹ Référentiel national d'identitovigilance, principes communs, juin 2022, chapitre 3.3.3.1.

⁵² Référentiel national d'identitovigilance, principes communs, juin 2022, chapitre 3.3.3.2.

⁵³ Règlement n°910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur.

⁵⁴ En application de l'article 1^{er} de la loi n° 2012-410 du 27 mars 2012 : « *l'identité d'une personne se prouve par tout moyen. La présentation d'une carte nationale d'identité ou d'un passeport français en cours de validité suffit à en justifier* ».

Annexe VI

Les professionnels de santé (médecins généralistes) soulignent qu'il serait plus simple que les mineurs aient leur propre carte, ne serait-ce que pour leur permettre de se présenter seuls, sans en avoir informé les parents et avoir dû demander leur carte Vitale (pour de la contraception / pilule du lendemain, par exemple).

Pour un syndicat de médecins, il faudrait simplifier la procédure de prise en charge (et lever un frein à l'accès aux soins) en gérant les mineurs par leur NIR.

Les responsables des services affiliation/facturation d'établissements de santé rencontrés par la mission considèrent qu'il s'agit d'un problème complexe qui génère d'importantes difficultés de prise en charge, notamment en cas de divorce (qu'il soit ou non conflictuel).

Il peut y avoir des écarts d'informations contenues entre les cartes Vitale des deux parents, faute de mise à jour, ce qui complique l'accès aux droits : un pharmacien rapporte par exemple le cas d'un mineur en « ALD »⁵⁵, mentionné sur l'une des cartes (et non sur l'autre) ; ou le cas récurrent de mineurs âgés de 16 ans en attente de leur carte Vitale pendant plusieurs semaines, sans n'être plus rattaché en tant qu'ayant-droit à un parent, et ne disposant pas des moyens financiers nécessaires pour avancer leurs frais de santé.

Deux CPAM interrogées considèrent que cette question est un point de difficulté de la carte Vitale, parce qu'elle fait l'objet de demandes spécifiques et récurrentes des usagers.

Les organismes complémentaires confirment qu'il s'agit d'un point de blocage parfois : le rattachement d'une mutuelle à la carte d'un seul parent sur les deux peut entraîner une rupture de la prise en charge du mineur, ou des rejets dans la chaîne de remboursements / facturations, qui sont compliquées à résoudre, si, de surcroît, les parents sont séparés.

Le nourrisson est, par ailleurs, à la naissance, dans la quasi-totalité des cas, rattaché uniquement à la carte Vitale de sa mère, ce qui décharge le père des visites chez le médecin (sauf en cas de prêt la carte Vitale de la mère de l'enfant). Le sujet est plus épineux encore lorsque l'enfant séjourne chez des tiers (à commencer par ses grands-parents) ou que les parents sont séparés, la question des avances de frais suivies de remboursements pouvant susciter des tensions entre ceux-ci.

Techniquement, inscrire le NIR sur la CNIe d'un enfant mineur ne devrait pas poser plus de difficulté que d'apposer celle d'un adulte majeur : le NIR d'un enfant est attribué dans les jours qui suivent la naissance, et figure sur les attestations de droits téléchargeables par exemple depuis un compte AMELI. Par ailleurs, en l'absence de CNIe de l'enfant, celle d'un parent permettrait de remonter, via la consultation des téléservices (voir *infra*) aux droits de l'enfant.

En toute hypothèse, et au-delà du scénario CNIe, le rattachement aux cartes Vitale des deux parents devrait être opérée dès la naissance de manière systématique de manière à favoriser une égale prise en charge des enfants.

3.3. La quasi-totalité de la population vivant en France disposera à terme d'un titre électronique sécurisé.

La détention d'une carte nationale d'identité n'est pas une obligation légale. En pratique, 97 % des Français ont une carte nationale d'identité⁵⁶.

⁵⁵ Affection de longue durée.

⁵⁶ Source : Ministère de l'Intérieur.

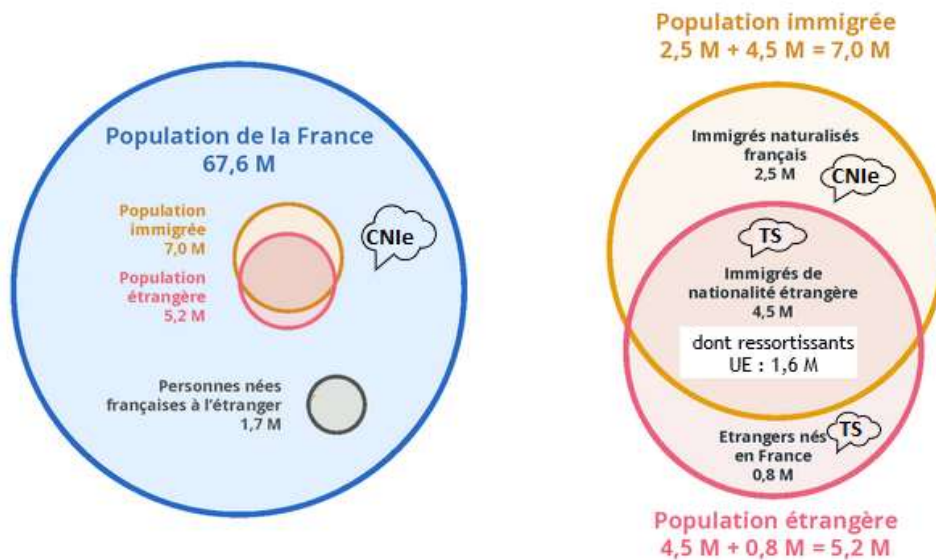
Annexe VI

La nouvelle carte électronique (CNIe) déployée depuis le 15 mars 2021 a adopté le format d'une carte bancaire et a été modernisée pour répondre aux impératifs de protection des données personnelles et aux standards de sécurité européens. Les données biométriques contenues dans la puce sont stockées « dans un compartiment hautement sécurisé et dont l'accès est spécifiquement encadré »⁵⁷. 6,6 millions de CNIe ont été établies en 2022, ce qui représente un renouvellement du parc sous dix années.

De même, le titre de séjour, uniformisé au niveau européen depuis 2011, a adopté le format de carte bancaire. À l'instar de la CNIe, il intègre une puce sans contact⁵⁸, des dispositifs de protection contre la falsification, une fonction d'identification électronique, et il permet d'apposer une signature ayant force obligatoire sur des documents numérisés.

À eux deux, ces titres sécurisés permettent de couvrir la quasi-totalité de la population vivant en France, y compris les ressortissants communautaires. En effet, ces derniers n'ont pas l'obligation de détenir un titre de séjour mais peuvent déposer une demande s'ils remplissent les conditions⁵⁹. Ils pourraient donc être incités à le faire s'ils souhaitent disposer d'une carte support pour leur NIR⁶⁰.

Graphique 5 : Couverture de la population vivant en France selon le lieu de naissance et la nationalité, dans le scénario d'un titre sécurisé porteur du NIR (2021)



Source : INSEE, estimations de la population, 2021.

⁵⁷ Source : Ministère de l'Intérieur.

⁵⁸ Communication en champ proche (CCP), plus connue sous son signe en anglais (NFC – near field communication).

⁵⁹ Cf. article L. 231-1 du code de l'entrée et du séjour des étrangers et du droit d'asile (les ressortissants suisses, islandais, lichtensteinois et norvégiens étant assimilés à des ressortissants communautaires en application de l'article L. 200-3 du même code).

⁶⁰ Pour les ressortissants communautaire, un scénario alternatif pourrait consister à leur demander de produire deux documents : leur titre d'identité national ainsi qu'une version simplifiée (non protégée, non électronique) de la carte Vitale, permettant seulement aux praticiens libéraux ou aux établissements de santé de lire le NIR. La présence du titre d'identité national serait alors également requise.

3.4. D'autres pays, notamment européens utilisent le support de la carte d'identité comme clé d'accès aux droits de l'assurance maladie

La mission a sollicité le réseau des conseillers pour les affaires sociales, ce qui lui a permis d'obtenir des précisions sur le dispositif mis en place à l'étranger (Danemark, Suède, Espagne, États-Unis). Le présent chapitre reprend les principaux éléments retournés à la mission⁶¹.

3.4.1. Portugal

Depuis 2007, le Portugal a mis en place une nouvelle « carte du citoyen », qui remplit la fonction de carte nationale d'identité et contient également le numéro de sécurité sociale et le numéro d'utilisateur de santé : le premier est utilisé pour l'identification et l'accès aux services de sécurité sociale et le second pour l'accès aux services de santé publique (hôpitaux, centres de santé, postes médicaux).

Tous les citoyens, dès leur naissance, disposent d'une carte de citoyen avec un numéro d'identification d'utilisateur civil, fiscal, sanitaire et de sécurité sociale. Des certificats électroniques d'authentification et de signature qualifiée (QDS), permettent aux usagers de s'authentifier auprès de services informatisés, à distance ou localement.

Le nombre de cartes physiques en circulation est 11 millions. Le nombre de cartes dématérialisées est de 650 0000 (soit un taux de couverture proche de 100 % des ressortissants).

La carte est présentée chaque rendez-vous, pour l'identification du patient. Elle est sécurisée par un code PIN. Sa durée de validité est de 10 années. Pour les nouveau-nés, elle est gratuite jusqu'à leurs 20 premiers jours. La puce n'est mise à jour que lors du renouvellement du document.

3.4.2. Danemark

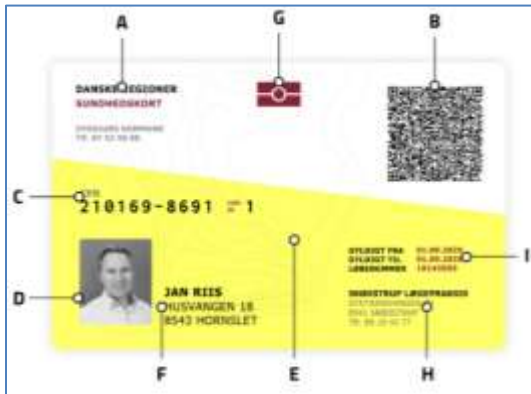
Les Danois disposent d'un numéro de sécurité sociale spécifique.

La carte de santé au Danemark (*Sundhedskort*) est disponible sous la forme d'un support physique (carte jaune, sans photo ni puce) ou au format dématérialisé (application mobile téléchargeable depuis le 1^{er} juin 2021).

⁶¹ À l'exception du chapitre consacré à la principauté de Monaco, rédigé par la mission.

Annexe VI

En 2019, un rapport⁶², dressant le constat que ce support ne permettait pas de s'assurer de l'identité du titulaire, et qu'il existait un « marché noir » des cartes jaunes, a recommandé de mettre en place à brève échéance « une nouvelle carte d'identité physique sécurisée par un QR code, un numéro de série et une option de blocage ». À plus long terme, il propose « la suppression complète de la carte de santé physique et numérique standard et son remplacement par une nouvelle carte d'identité nationale sécurisée (physique et numérique) avec l'obligation d'une photo ou de mesures similaires pour vérifier que l'individu qui présente la carte est bien son détenteur réel. [...] Cette carte (physique ou numérique) doit être présentée lors des rendez-vous avec les prestataires de soins de santé ».



Cette nouvelle carte d'identité aurait vocation à remplacer plusieurs cartes ou titres préexistants (CNI, permis de conduire, carte de santé).

3.4.3. Belgique

En Belgique, il n'existe pas de numéro de sécurité sociale spécifique. Un identifiant unique est utilisé par plusieurs administrations et services publics. En 2014, la carte d'identité électronique a pris en charge les fonctionnalités de la carte SIS (système d'information sociale). Cette dernière, électronique depuis 2004, permettait à ses détenteurs de s'authentifier et de signer numériquement des documents.

Depuis septembre 2021, la prescription électronique est intégrée à la carte d'identité électronique (le patient pouvant toujours opter pour la prescription papier).

Une autre carte est délivrée aux assurés sociaux qui n'ont pas de carte d'identité électronique belge (ressortissants communautaires...) : la carte « isi+ ».

Par ailleurs, le contrôle d'identité des patients par les infirmiers est obligatoire depuis octobre 2017. Dans le secteur hospitalier, l'obligation de procéder à un contrôle d'identité entrera en vigueur en janvier 2024.

3.4.4. Suède

En Suède, il n'existe pas de carte d'assurance maladie. Il n'existe pas d'identifiant spécifique à l'assurance maladie, mais un numéro personnel (*personnummer*) stocké sur la carte d'identité et le permis de conduire.

Les professionnels de santé ont l'obligation réglementaire de s'assurer à chaque fois de l'identité du patient. Le contrôle doit avoir lieu sur présentation d'une pièce d'identité approuvée. La quasi-majorité des personnes adultes présentent leur permis de conduire comme pièce d'identité, systématiquement à chaque visite, ou leur carte d'identité⁶³.

⁶² « Une carte de santé plus sûre », cabinet de conseil en IT Lakeside et commandé par le ministère de la Santé et les régions danoises, 2019.

⁶³ Réseau des conseillers aux affaires sociales.

3.4.5. Allemagne

En Allemagne, la carte de santé électronique (*eGK*) ne comprend pas de donnée biométrique. Les cartes qui disposent d'une fonction NFC sécurisent l'accès aux données par un code PIN.



La carte de santé électronique comprend au recto :

- ◆ les données administratives de l'assuré, (le nom, la date de naissance et l'adresse ainsi que des informations sur l'assurance maladie, telles que le numéro d'assurance maladie et le statut d'assuré (membre, membre de la famille ou retraité) ;
- ◆ une photographie (sauf pour les mineurs de moins de 15 ans et pour les personnes en situation de handicap).

Le verso de la carte peut être utilisé par les compagnies d'assurance maladie comme carte européenne d'assurance maladie.

La carte peut également contenir des données médicales et personnelles uniquement si le patient y consent :

- ◆ Les données d'urgence : informations sur l'intolérance aux médicaments, les allergies et les maladies chroniques, qui peuvent être importantes à connaître pour un traitement en cas d'urgence, stockées numériquement sur leur *eGK* en tant que données d'urgence ; L'accès aux données d'urgence est sans code PIN possible pour les médecins via leur carte professionnelle de santé électronique (*eHBA*) ;
- ◆ un plan de médication pour prévenir les interactions potentiellement mortelles dans le cadre des soins courants, en dehors des soins d'urgence aiguë (accès via code PIN) - En Allemagne, ces données ont été rendues disponibles après avoir fait le constat qu'environ 5 à 10 % de toutes les admissions à l'hôpital sont dues à des réactions indésirables aux médicaments, et qu'un quart de celles-ci pourraient être évitées (soit à l'échelle du pays environ 250 000 à 500 000 hospitalisations par an dues à des erreurs de médication évitables) ;

depuis le 1er octobre 2016, les patients qui utilisent au moins trois médicaments prescrits en même temps et pris sur une période d'au moins 28 jours ont le droit de faire établir et délivrer par leur médecin traitant un plan de médication. Ce plan peut être consulté par les médecins (parcours patient) et les pharmaciens lors de la distribution de médicaments en officine ;

- ◆ des informations personnelles sur l'existence d'une déclaration écrite de don d'organes et de tissus, d'un testament de vie ou d'une procuration et leur lieu de stockage (par exemple "dans le tiroir du bureau de gauche ") peuvent être stockés sur l'*eGK* (accès via code PIN).

En Allemagne, les données contenues sur la carte de santé peuvent être mises à jour à chaque visite chez un médecin généraliste (qui est rémunéré à cet effet).

Les assurés peuvent désactiver l'usage du code PIN.

3.4.6. Espagne



En Espagne, la carte de santé adopte le format d'une carte de crédit. Elle comporte un numéro d'identification unique, propre à chaque citoyen et au système national de soins. Ce numéro est délivré, au niveau national, par le ministère de la santé. Elle intègre une puce et un QR code (cf. photo ci-dessous).

La carte donne accès au dossier médical du patient⁶⁴.

3.4.7. États Unis

Aux États Unis, « la question du passage à une carte électronique avec le cas échéant des éléments d'authentification complémentaire (photo ou biométrie) a fait l'objet d'une étude approfondie en 2015 du Government Accountability Office « Medicare- Potential Uses of Electronically Readable Cards for Beneficiaries and Providers » ([qao-15-319.pdf](#)). Ce rapport s'est notamment fondé sur des échanges avec les administrations française et allemande pour évaluer les bénéfices et les coûts induits par la mise en place d'une carte « électronique ». (...)

Ses conclusions se sont avérées négatives (...) [en raison du] coût organisationnel de mise en place, [des] coûts de fonctionnement d'un système de carte type carte vitale, [des] craintes que ce dispositif entrave l'accès aux soins de publics fragiles, [des] risques de fraude résiduelle élevée (...) [et du] risque de limiter l'accès aux soins »⁶⁵.

La biométrie a fait l'objet de plusieurs expérimentations dans le domaine de la santé au niveau local. Les empreintes digitales sont principalement utilisées dans le milieu hospitalier (connexion des médecins à leur poste de travail). Deux expériences sont présentées dans le système hospitalier : le déploiement de scans biométriques (reconnaissance de l'iris et du visage) par le plus grand prestataire de soins dans l'État de New York (Northwell Health), et de scanners d'empreintes digitales au centre médical de l'Université de Pittsburgh (UPMC) mis en place en 2016 pour réduire le temps d'enregistrement des patients.

À noter qu'un contrôle d'identité du prescripteur est mis en place lors de la délivrance de produits stupéfiants : « Une loi fédérale récente (2021) visant à lutter contre l'abus de prescription d'opioïdes exige que les médecins envoient aux pharmacies des ordonnances numériques, et non en papier, pour les substances contrôlées et qu'ils se conforment aux règles et normes de la Drug Enforcement Administration (DEA). **La DEA exige une authentification à deux facteurs pour authentifier l'identité du prescripteur. Les prescripteurs saisissent un code aléatoire généré par un badge disponible, puis un lecteur authentifie l'identité de la personne et son autorisation de prescrire** »⁶⁶.

⁶⁴ Réseau des conseillers aux affaires sociales.

⁶⁵ Réseau des conseillers aux affaires sociales.

⁶⁶ Réseau des conseillers aux affaires sociales.

3.5. Le NIR pourrait être embarqué sur la CNIe et les titres de séjour

Le NIR pourrait être inséré sur la CNIe selon deux modalités :

- ◆ en puce, dans un container dédié à la sphère sociale et accessible seulement par celle-ci (cf. 3.5.1) ;
- ◆ sur le 2D-DOC figurant au verso de la CNIe (cf. 3.5.2).

En toute hypothèse, les données issues de la sphère régaliennne et de la sphère sociale ne devraient être jointes qu'aux dernières étapes du processus d'établissement de la CNIe (3.5.3).

3.5.1. La CNIe pourrait disposer d'un *container* dans sa puce permettant de communiquer le NIR aux professionnels de santé

Dans ce scénario, le NIR est intégré dans un compartiment ou *container* spécifique à l'assurance maladie, intégré à la puce.

D'après l'ANTS et l'Imprimerie nationale, l'ajout d'un nouveau compartiment (ou *container*) dans la puce intégrée dans la CNIe ou dans le titre de séjour ne présente pas de difficulté technique particulière ou de problème de capacité de mémoire. Ces éléments devront toutefois être confortés par une étude de faisabilité détaillée.

Ce *container* (qui devra être sécurisé au niveau adapté à la sensibilité attachée au NIR⁶⁷) serait lisible uniquement par les personnes habilitées, à l'instar de la carte Vitale (professionnels de santé, services de l'Assurance maladie), et ne serait pas accessible en écriture.

Ce compartiment n'aura en effet plus besoin d'être mis à jour régulièrement, contrairement à la carte Vitale actuelle. Il ne contiendra pas les données relatives à l'ouverture des droits. En effet, les droits seraient communiqués au professionnel ou établissement de santé par l'interrogation, sur la base du NIR ainsi obtenu, des téléservices ADRI (pour les professionnels libéraux) ou CDRI (établissements de santé). La disponibilité et la fiabilité de ces téléservices est donc clé dans ce scénario ; il convient toutefois de remarquer que l'accès au téléservice ADRI conditionne de la même manière la mise en œuvre de l'application carte Vitale. Ce téléservice est actuellement appelé via les logiciels des éditeurs (793 millions d'appels ADRI en 2022, 70 millions d'appels CDRI, 316 millions de consultations CDR d'après le GIE SESAM Vitale).

Ce *container* serait séparé de façon étanche de l'identité régaliennne avec impossibilité pour les services du ministère de l'Intérieur de le lire. La lecture du container pourrait être conditionnée, par exemple, à une authentification par la carte CPS (pour un professionnel de santé) ou CPE (pour les services administratifs d'un établissement de santé), dans leurs versions physique ou dématérialisée.

L'accès à la puce de la CNIe est réglementé⁶⁸ : une évolution des textes serait donc nécessaire, associée à un travail de communication afin d'expliquer les garanties de sécurité et d'intégrité mises en œuvre.

⁶⁷ Alors même que le NIR n'est pas une donnée sensible au sens du RGPD, la CNIL estime qu'il s'agit d'une donnée devant faire l'objet d'une protection particulière.

⁶⁸ Décret n° 2016-1460 du 28 octobre 2016 autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité. La France est le seul pays de l'Union à limiter le nombre des accédants.

3.5.2. La CNIE pourrait afficher le NIR dans le 2D-DOC présent à son verso

Dans ce scénario, le support du NIR n'est plus la puce mais le QR code 2D-DOC figurant au verso de la nouvelle carte nationale d'identité (entouré en vert dans le graphique 6) :

Graphique 6 : Verso d'une CNIE



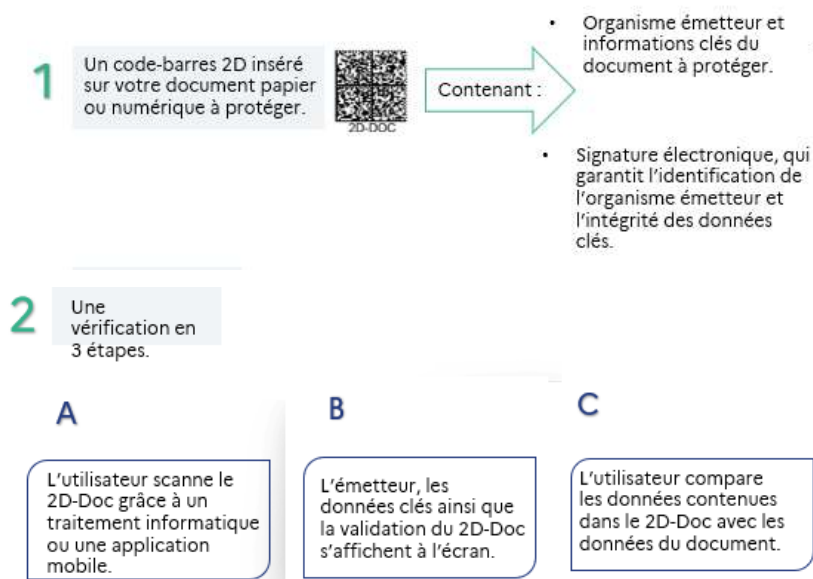
Source : Ministère de l'Intérieur – mission pour les encadrés vert et marron.

La sécurisation est garantie par la chaîne de confiance associant l'éditeur de lecteur, l'autorité de certification et le ministère de l'Intérieur.

La vérification de l'authenticité et les informations clés du document seront accessibles par un simple scan avec un lecteur conforme 2D-DOC (cf. graphique 7). Seul un lecteur conforme vérifie le certificat qui garantit l'authenticité des données et respecte la confidentialité de l'utilisateur.

Les professionnels de santé, qui seront prochainement équipés d'une douchette dans le cadre de la généralisation de l'application carte Vitale, scanneront le 2D-DOC qui servira de clé d'accès au téléservice ADri/CDRi.

Graphique 7 : Schéma de fonctionnement du dispositif 2D-DOC



Source : Mission d'après ministère de l'Intérieur.

Comme l'indique la direction du management de l'administration territoriale et de l'encadrement supérieur du ministère de l'Intérieur, cette solution est :

Annexe VI

- ◆ simple et peu coûteuse à intégrer sur un document susceptible d'être fraudé ;
- ◆ facile à vérifier sur format papier et format numérique ;
- ◆ sécurisé par signature électronique et piloté par le Ministère de l'Intérieur ;
- ◆ respectueuse du RGPD.

Elle figure d'ores et déjà sur la carte nationale d'identité, la carte sapeurs-pompiers, certains justificatifs de domicile, les attestations vaccinales, le pass sanitaire, le certificat de qualité de l'air (vignette Crit'Air).

Toutefois le 2D-DOC ne figure pas encore sur le titre de séjour.

Au-delà, le dispositif 2D-DOC pourrait constituer une piste de sécurisation de l'attestation de droits papier.

3.5.3. Le NIR devrait être traité par l'Imprimerie nationale de manière sécurisée

L'Imprimerie nationale, qui dispose d'ores et déjà d'un monopole pour la réalisation des cartes de professionnel de santé⁶⁹ se verrait confier l'intégration du NIR dans la puce des CNI et des titres de séjour sécurisés, pour lesquels elle dispose également d'un monopole d'impression⁷⁰.

Il s'agit de s'assurer de la **complète séparation des canaux liés à l'identité régalienn e et à l'identité sociale incarnée par le numéro de sécurité sociale** (le NIR). Ainsi, afin de s'assurer de leur parfaite étanchéité, il conviendrait que les deux informations ne soient jointes qu'au moment de la personnalisation de la CNIe, soit dans les dernières étapes du processus d'établissement du titre, et que les personnels en charge de cette tâche soient soumis à des obligations de secret professionnel renforcées sur ce point.

Afin de maintenir ces **canaux séparés**, le traitement de récupération de la donnée NIR s'effectuerait à partir d'un téléservice spécifique (similaire au téléservice INSi⁷¹) permettant à l'Imprimerie nationale, à partir du NIR renseigné par le demandeur lors du dépôt de la demande de CNIe, de procéder à la vérification de l'existence du NIR et à des contrôles de cohérence entre le NIR stocké dans le RNIPP/SNGI (qui est un identifiant signifiant) et les informations contenues sur la demande (par exemple si sexe indiqué est masculin, le NIR commence bien par 1).

La détention d'une carte Vitale n'est pas obligatoire. De même, l'utilisateur qui demande le renouvellement de son titre sécurisé aura la possibilité de refuser l'intégration du NIR⁷² dans la CNIe, simplement en ne renseignant pas la zone prévue sur le formulaire de dépôt de la demande⁷³. Il lui reviendra, comme cela est déjà le cas actuellement, de justifier de l'ouverture de ses droits à la sécurité sociale par tout autre moyen (application carte Vitale, attestation de droits papier accompagnée éventuellement de la présentation d'un titre d'identité comprenant une photographie).

⁶⁹ Décret n° 2012-1117 du 2 octobre 2012 relatif à l'intégration de la carte de professionnel de santé dans le monopole de l'Imprimerie nationale.

⁷⁰ Décret n°2006-1436 du 24 novembre 2006 pris pour l'application de l'article 2 de la loi n° 93-1419 du 31 décembre 1993 relative à l'Imprimerie nationale

⁷¹ Le téléservice INSi (Identifiant National de Santé intégré) permet aux acteurs de la santé et du médico-social d'obtenir l'Identité Nationale de Santé (INS) d'un patient/usager.

⁷² Il est également possible, s'il est né à l'étranger et n'a jamais été immatriculé à la sécurité sociale française que, bien que citoyen français, il ne dispose pas de NIR.

⁷³ Formulaire électronique préétabli en ligne ou formulaire papier.

3.6. Les téléservices de consultation des droits doivent être fiables et disponibles

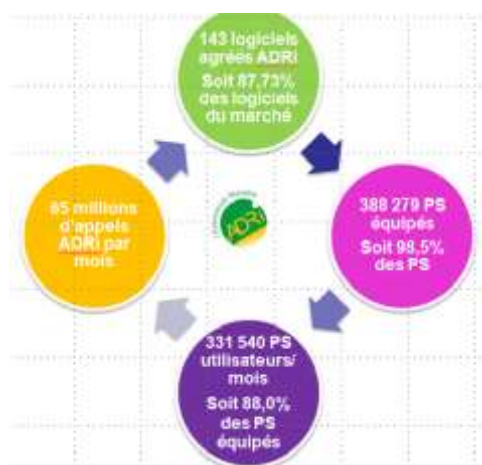
Que le NIR soit obtenu à travers la puce de la CNIe ou de son 2D-DOC, les droits à la prise en charge des frais de santé ne sont plus inscrits en carte comme c'est le cas avec la carte Vitale actuelle. Elle ne sert que de clé d'entrée pour accéder au téléservice adéquat. Cette architecture est actuellement en place et est celle qui est utilisée dans le cadre du déploiement de l'application carte Vitale (cf. voir annexe IV).

D'ores et déjà, les téléservices qui permettent d'accéder en temps réel aux droits ouverts à l'assurance maladie (ADRI/CDRI) sont déployés dans la majorité des cabinets, la quasi-totalité des pharmacies d'officine et des établissements de santé. Suivant la manière dont ils sont paramétrés, ils sont appelés de manière systématique ou de manière plus épisodique (en particulier lorsqu'un patient, déjà connu, se présente en cabinet sans sa carte Vitale).

Dans les deux cas, le matériel mobilisé par les professionnels et établissements de santé est identique à celui nécessaire pour lire les données de l'application carte Vitale (ou ApCV) : un lecteur NFC pour le NIR en puce ou une douchette pour le NIR sur 2D-DOC seront utilisés par l'application carte Vitale.

À ce jour, seule l'utilisation de la carte Vitale offre une garantie de paiement au professionnel ou à l'établissement, quand bien même le téléservice ADRI/CDRI, afficherait des écarts avec l'information en carte⁷⁴.

Graphique 8 : Chiffres clés du téléservice ADRI (novembre 2022)



Source : GIE SESAM Vitale.

Les éléments communiqués par l'Assurance maladie confirment que le recours au téléservice ADRI permet de réduire sensiblement le taux de rejet, tous flux de facturation confondus (dégradés, non dégradés), et en particulier de diviser par 2 le taux de rejet des factures réalisées avec une carte Vitale (cf. éléments détaillées dans l'annexe relative à l'application carte Vitale).

S'agissant du scénario « NIR sur la carte d'identité », il convient de conduire une étude de faisabilité détaillée pour :

⁷⁴ Les droits en carte font foi et font même l'objet d'une garantie de paiement. Toutefois, lorsque le professionnel de santé, simultanément, utilise la carte Vitale et consulte les droits sur ADRI, ce sont les droits les plus élevés qui sont retenus.

Annexe VI

- ◆ déterminer le besoin de modification des spécifications des téléservices ADRI / CDRI pour réaliser un appel à partir du NIR uniquement. A l'heure actuelle, ces téléservices demandent en outre le code régime de l'assurance maladie obligatoire, la date de naissance du bénéficiaire de soins et son rang de naissance : ces dernières données étaient obligatoires dès lors qu'à un même NIR pouvaient être rattachés plusieurs ayants-droits⁷⁵. Si les titres sécurisés deviennent le support de droits individualisés, ces données deviendraient facultatives ;
- ◆ améliorer le taux de disponibilité des deux téléservices (de l'ordre de 94 %-98 % pour ADRI, 90 %-95 % pour CDRI selon les mois⁷⁶) par des travaux sur l'infrastructure et/ou par la mise en place d'outils de supervision ;
- ◆ valider les capacités de montée en charge de l'architecture du réseau et des infrastructures associées ;
- ◆ corriger les difficultés rencontrées actuellement dans ADRI en termes d'exactitude des informations renvoyées par le téléservice (voir encadré) ;
- ◆ étudier la nécessité de mettre en place une procédure de secours pour garantir la facturation, y compris dans l'hypothèse d'indisponibilité du téléservice ADRI/CDRI ou lors des déplacements chez des patients isolés (zone blanche ou connexion réseau défaillante)⁷⁷, sauf à maintenir le recours à des flux dégradés, ce qui est le cas aujourd'hui avec les feuilles de soins papier.

Encadré 5 : Les limites du téléservice ADRI

Le téléservice ADRI (Acquisition des droits intégrée) permet, en temps réel, de consulter les droits d'un assuré social, quel que soit son régime d'appartenance. Ce téléservice est intégré au sein des solutions logicielles des professionnels de santé, qui peuvent consulter, sur la base du NIR du patient, l'étendue de ses droits.

En théorie, les droits affichés par ADRI sont de la même nature que ceux inscrits sur la carte Vitale. Ainsi, si la mention d'une ALD est bien présente sur ADRI, sa nature n'est pas précisée et le professionnel de santé devra consulter le portail Ameli-pro afin de la connaître.

Deux difficultés viennent toutefois entraver le bon fonctionnement de ce service :

La disponibilité du service est parfois limitée. En octobre 2022, 3,5% des requêtes avaient échoué sans qu'une anomalie expliquant cet échec – par exemple l'assuré n'existe pas en base – soit identifiée (ce taux dépassant 90% s'agissant des anciens ressortissants du RSI).

L'exhaustivité des données transmises est parfois défaillante, ce qui pose notamment problème aux pharmaciens. À titre d'illustration, à l'occasion de la réunion de la commission paritaire locale de Saône et Loire du 24 mars 2022, la section professionnelle des pharmaciens relève « *qu'ADRI ne permet pas de gérer deux exonérations* », générant ainsi des rejets. Dans le même cadre mais dans la Côte d'Or, un membre la section professionnelle indiquait, lors de sa réunion du 17 octobre 2022, que « *lorsque l'assuré est en invalidité et en ALD, ADRI ne gère que l'ALD. Pour les soins hors ALD, le pharmacien facture alors avec application du ticket modérateur. Or, la facture est rejetée car elle aurait dû être facturée à 100% au titre de l'invalidité* ». Le relevé de décision indique qu'une « *nouvelle remontée sera faite à la CNAM* ».

Le téléservice ADRI est intégré à bord de l'application carte Vitale (ApCV) : les droits affichés par ADRI (appel du logiciel métier du praticien) sont identiques à ceux fournis par l'ApCV.

Source : Mission.

⁷⁵ Ces données peuvent être récupérées de la base patient.

⁷⁶ DDGOS/DSMOI/DSV, novembre 2022.

⁷⁷ Point soulevé par les professionnels de santé.

3.7. La CNIe ou le titre de séjour devrait permettre, dans ce scénario, la signature de feuilles de soin électroniques

Dernière fonctionnalité de la carte Vitale, la signature de FSE doit également être permise par la CNIe ou le titre de séjour.

Dans le cas de l'inscription du NIR en puce, la présence de la CNIe est assurée par la présence de sa puce (qui s'est nécessairement authentifiée auprès du système du professionnel ou de l'établissement de santé avant de délivrer le NIR qu'elle renferme) : le modèle est donc le même que celui de la carte Vitale actuelle, la signature de la FSE étant effectuée, côté assuré, par la présence de la CNIe en mode sans contact.

Dans le scénario où le NIR est inscrit dans le 2D-DOC, une deuxième opération est nécessaire pour le professionnel ou l'établissement de santé : il convient alors de s'assurer de la présence de la CNIe ou du titre de séjour en lisant la bande MRZ (voir Graphique 6, en marron) qu'il contient.

Dans le cas des ressortissant européens, la bande MRZ⁷⁸ de leur document d'identité est en théorie standardisée et lisible par un dispositif français. Il est donc en principe, sous réserve d'une étude plus approfondie, de s'assurer de la présence d'un document d'identité communautaire aux fins de signature de la FSE.

3.8. La montée en charge du déploiement de la solution CNIe sera liée au renouvellement et à la mise à niveau du parc de cartes d'identité

En 2021, l'ANTS a fabriqué 12,1 millions de titres sécurisés, dont 6,6 millions de CNIe et 5,5 millions de passeports (+ 30 % depuis 2019).

Dans ce scénario, le déploiement est progressif, au fur et à mesure de la généralisation de la nouvelle carte d'identité. Il s'appuie sur les procédures déjà mises en place de délivrance et de renouvellement des titres électroniques.

D'après IN Groupe, il serait par ailleurs possible de déployer ce *container a posteriori* dans la majorité des puces pour les titres précédemment émis en 2021-2022 (soit dans 6 à 7 millions de titres)⁷⁹.

D'après l'ANTS, dans 30 % à 40 % des cas, les demandes de titres concernent les mineurs, pour qui il s'agit d'une première demande pour la moitié d'entre eux (15 % des autres demandes étant des demandes de renouvellement, les autres demandes se répartissant entre motifs personnels, changements d'état civil ou d'adresse).

3.9. Les professionnels de santé et établissements de santé interrogés sont favorables : ils y voient une source de simplification administrative et de sécurisation des soins

Cette solution, parfois évoquée spontanément par nos interlocuteurs, fait consensus. L'ensemble des professionnels de santé interrogés (cf. liste en annexe), les syndicats représentants des professions de santé, les ordres, les assureurs complémentaires, les fédérations d'établissements de santé n'ont pas exprimé d'opposition au scénario d'inclusion du NIR à la carte nationale d'identité, voire expriment souvent un soutien à une telle solution :

⁷⁸ Machine readable zone ou zone de lecture automatique (ZLA) en français. Toutes les cartes d'identité communautaires doivent en comprendre une, établie selon la norme (aéronautique) spécifiée dans le document 9303 de l'OACI.

⁷⁹ Possibilité pour environ deux tiers des nouvelles cartes d'identité d'ores et déjà émises (env. 10 millions).

Annexe VI

- ◆ ils considèrent que la carte Vitale physique est une technologie robuste et solide mais qui a fait son temps : mettre le NIR dans la CNiE est apparu à plusieurs interlocuteurs comment une idée séduisante, complémentaire à la généralisation de l'application carte Vitale ;
- ◆ les professionnels soulignent que la présentation systématique de la carte d'identité leur permettrait de remplir naturellement, au cours des soins, leur obligation en matière d'identitovigilance ;
- ◆ les patients oublient ou égarent probablement moins souvent leur carte d'identité que leur carte Vitale ;
- ◆ la lecture de la CNiE à distance règle le problème de lecture d'une puce usée ;
- ◆ certains ont même indiqué à la mission que ce serait un moyen d'appuyer les efforts entrepris ces dernières années pour renforcer l'identitovigilance ;
- ◆ Le conseil national de l'ordre des infirmiers insiste également sur la nécessité d'y insérer les données d'urgence et les directives anticipées.

Par ailleurs, deux des trois caisses primaires d'assurance maladie interrogées (la troisième n'ayant pas été interrogée à ce sujet) se sont prononcées également de manière très positive en faveur de la généralisation du téléservice ADRI / CDRI dans une perspective de simplification des flux de facturation et de réduction du nombre de rejets carte Vitale du fait des problèmes de mise à jour.

3.10. La CNAM a émis de très fortes réserves, qui paraissent pouvoir être levées

Le directeur général de l'Assurance maladie a toutefois fait part de ses « *très fortes réserves* », dans un mail (cf. pièce jointe en annexe IX) concernant ce projet, aux motifs que ce projet:

- ◆ **ne répondrait à aucun besoin ou enjeu, en termes de lutte contre la fraude ou en termes de simplification administrative ;**
 - il semble cependant à la mission que l'inscription du NIR sur des titres sécurisés officiels, en plus de rendre les fraudes à l'usurpation d'identité plus difficiles, permet de réduire le nombre de justificatifs physiques des usagers dans leurs démarches quotidiennes ;
 - pour les professionnels de santé, notamment en ville, il permet de qualifier l'INS dans une optique de sécurité sanitaire, tout en donnant accès aux droits à jour de l'assuré ;
- ◆ **pourrait fragiliser le déploiement de l'ApCV ;**
 - pour la mission, le développement puis déploiement d'un tel projet ne pourrait intervenir – et n'aurait de sens – qu'après la généralisation réussie de l'application carte Vitale, en séparant bien les deux temporalités ;
 - par ailleurs, il semble à la mission que ce scénario s'inscrirait en pleine complémentarité avec l'ApCV, en offrant la possibilité aux usagers de posséder un support physique alternatif à l'application (lorsque l'utilisateur ne possède pas de smartphone, qu'il n'a pas souhaité installer l'appliquatif, ou que son smartphone est déchargé, voire volé) ;
- ◆ **ne permettrait pas de couvrir à lui seul l'ensemble de la population assurée ;**
 - effectivement, c'est pourquoi la mission recommande de conserver le maintien d'au moins deux supports des droits (application dématérialisée et titres sécurisés) en plus de l'attestation de droit en format papier ;
- ◆ **soulèverait des risques techniques ;**

Annexe VI

- les premières investigations de la mission montrent que l'architecture technique de l'application carte Vitale pourrait être utilement réutilisée pour le scénario du NIR sur la pièce d'identité, moyennant plusieurs développements informatiques ;
- ◆ **souleverait des difficultés en termes de communication avec les assurés si ces derniers ne disposent pas du NIR sur la CNiE ;**
 - la mission rappelle que tout comme la détention d'une carte Vitale ou de l'application carte Vitale n'est pas obligatoire, la détention d'un titre sécurisé intégrant le NIR ne serait en aucun cas obligatoire ; les assurés pourraient continuer à justifier de leurs droits au moyen d'une attestation en format papier ;
- ◆ **risquerait de soulever des inquiétudes politiques du fait de la juxtaposition sur un même support de données d'état civil et du NIR ;**
 - la mission estime que ce risque peut être minoré dès lors que l'étanchéité de l'implémentation des containers « Intérieur » et « Assurance maladie » peut être garantie sur la puce et contrôlé par la CNIL, et que cette implantation d'un container « Assurance maladie » reste facultative et soumise à un consentement explicite de l'utilisateur.

3.11. Les conditions pré-requises à la réalisation d'un tel scénario, listées par la CNIL, paraissent pouvoir être remplies, sous réserve d'une étude approfondie.

Interrogées par la mission sur ces différents scénarios, la CNIL, dans sa réponse à la mission (cf. Annexe VII), note que le « scénario visant à intégrer le NIR sur la puce constitue donc la solution la moins intrusive et la moins risquée d'un point de vue technique. Cette solution nécessiterait, en tout état de cause, la réalisation d'une étude technique, juridique et économique poussée, qui devra impliquer les mesures décrites ci-dessous :

- ◆ *assurer le cloisonnement du NIR par rapport aux autres données contenues dans la puce de ces titres et leurs usages, notamment en chiffrant le conteneur « assurance maladie » de manière spécifique et lisible uniquement par les outils et acteurs de la sphère médicale et médico-sociale. En effet, le règlement (UE) 2019/1157 permet aux États membres d'intégrer sur la puce d'un titre d'identité ou de séjour d'autres données que celles nécessaires à la preuve de l'identité du titulaire. Ce même texte impose, néanmoins, que ces autres données soient physiquement ou logiquement séparées des données biométriques ;*
- ◆ *mettre en œuvre des mesures particulières de sécurité pour assurer le cloisonnement du NIR tout au long de la procédure de création et de délivrance du titre afin de ne pas communiquer aux services de mairie et de préfecture cet identifiant, si besoin en ayant recours à un tiers de confiance ;*
- ◆ *prévoir l'application du secret professionnel aux accédants du NIR aux fins de création et de délivrance des titres d'identité destinés à le porter ;*
- ◆ *inscrire au niveau de la loi le droit de tout assuré à s'opposer au traitement du NIR sur son titre d'identité ou de séjour ;*
- ◆ *s'assurer que des alternatives soient maintenues pour qu'un assuré puisse prouver ses droits et bénéficier de la prise en charge par l'assurance maladie. Ces alternatives ne devront pas conduire à une stigmatisation des personnes ne disposant pas de leur titre d'identité ou de limitation quant à l'accès aux soins ».*

Annexe VI

La mission partage l'avis de la CNIL, s'agissant de la nécessité de réaliser une étude de faisabilité approfondie, tant juridique que technique, pour procéder notamment aux réflexions complémentaires nécessaires « *pour tenir compte du caractère non obligatoire de détention d'une CNle, de l'absence de titre de séjour pour les personnes étrangères mineures ou encore la situation particulière des ressortissants des autres pays de l'Union européenne* »⁸⁰. Sans préempter ses conclusions, en l'état des travaux de la mission, l'ensemble des mesures pré-requises semblent pouvoir être remplies et peuvent trouver une solution juridique ou technique de nature à les satisfaire.

⁸⁰ Cf. courrier de la CNIL à la mission du 13 mars 2023 en annexe VII.

ANNEXE VII

Analyse juridique

SOMMAIRE

1. LA MISE EN PLACE D'UNE CARTE VITALE BIOMÉTRIQUE DOIT SE FAIRE DANS LE RESPECT DU PRINCIPE DE PROPORTIONNALITÉ1
2. LE SYSTÈME BIOMÉTRIQUE DOIT PERMETTRE UNE ALTERNATIVE POUR LES ASSURÉS SOCIAUX QUI NE PEUVENT, POUR DES MOTIFS LÉGITIMES, Y ÊTRE ASSUJETTIS.....2
 - 2.1. Le système biométrique ne doit pas interdire à des assurés sociaux d'exercer leurs droits.....2
 - 2.2. Le système alternatif doit présenter des garanties équivalentes3

Annexe VII

Cette annexe présente les principaux enseignements des éléments que la mission a obtenus auprès :

- ◆ de la Commission nationale de l'informatique et des libertés (CNIL), dans son avis du 13 mars 2023 (pièce jointe n°1) ;
- ◆ de la Direction des affaires juridiques des ministères chargés des affaires sociales, dans ses réponses du 24 mars 2023 au questionnaire de la mission (pièce jointe n°2).

Dans les deux cas, la difficulté de se prononcer de manière générale, sans qu'une architecture fine soit présentée, est soulignée. C'est la conséquence logique du cadrage large de la lettre de mission.

Pour autant, de grandes lignes de force se dessinent :

- ◆ aucun principe constitutionnel ni aucune règle de droit européen ne s'oppose à la mise en place d'une carte Vitale biométrique ;
- ◆ toutefois, une attention particulière doit être portée aux principes de nécessité et de proportionnalité : il s'agit de vérifier que la mise en place d'une carte Vitale biométrique, qui suppose une atteinte potentiellement significative au droit à la vie privée, peut être justifiée par des gains substantiels en termes de lutte contre la fraude. question est, de fait, préliminaire à toute autre. Ainsi, si les gains en termes de lutte contre la fraude s'avéraient mineurs, la solution biométrique verrait son fondement juridique (article 9 du RGPD notamment) fortement amoindri et encourrait avec une forte probabilité une censure du juge ;
- ◆ par ailleurs, des difficultés particulières apparaissent concernant les personnes ne pouvant pas, pour des motifs légitimes, être enrôlés dans le système. De plus, les personnes non reconnues par le système (faux négatifs) doivent disposer d'un moyen d'identification alternatif leur permettant d'exercer leurs droits.

1. La mise en place d'une carte Vitale biométrique doit se faire dans le respect du principe de proportionnalité

Le Conseil constitutionnel a rappelé dans sa décision DC 2012-652 du 22 mars 2012 que « *la liberté proclamée par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 implique le droit au respect de la vie privée ; que, par suite, la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif* ». Ainsi, l'existence d'un motif d'intérêt général, qui ne pose pas de difficulté dans le cas de la carte Vitale biométrique, est nécessaire mais pas suffisant. Il doit être complété par une mise en œuvre proportionnée.

On retrouve d'ailleurs un objectif équivalent dans les textes européens. En effet, l'article 9 du règlement 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (dit RGPD) prévoit une interdiction générale du « *traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique* ». Le même article prévoit toutefois toute une série d'exceptions à cette interdiction, dont celle organisée au 9.2.b du RGPD lorsque « *le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale, dans la mesure où ce traitement est autorisé par le droit de l'Union, par le droit d'un État membre ou par une convention collective conclue en vertu du droit d'un État membre qui prévoit des garanties appropriées pour les droits fondamentaux et les intérêts de la personne concernée* ».

S'il devait être saisi, le juge devrait donc mettre en balance :

Annexe VII

- ◆ d'une part, les résultats obtenus en regard de l'objectif poursuivi : la lutte contre la fraude dans ce cas ;
- ◆ et d'autre part l'intensité de l'atteinte à une liberté fondamentale : ici, le droit à la vie privée.

Par conséquent, la mise en place d'une carte Vitale biométrique devrait être justifiée par des gains substantiels en termes de lutte contre la fraude.

2. Le système biométrique doit permettre une alternative pour les assurés sociaux qui ne peuvent, pour des motifs légitimes, y être assujettis

Les assurés sociaux ne peuvent pas être privés par le système biométrique de l'exercice de leurs droits, ce qui conduit à l'adoption de solutions alternatives mobilisables pour des raisons légitimes, comme l'impossibilité physique de participer au système biométrique, la distance au système social ou la complexité de celui-ci par exemple (2.1). Le système alternatif doit alors présenter des garanties équivalentes : dans le cas contraire, les fraudeurs y auraient recours plutôt qu'au système biométrique, diminuant ainsi les gains obtenus par le système biométrique (2.2).

2.1. Le système biométrique ne doit pas interdire à des assurés sociaux d'exercer leurs droits

Dans un arrêt récent¹ relatif aux demandes de titres de séjour par les étrangers, le Conseil d'État a affirmé :

- ◆ qu'il était, en toute généralité, loisible au pouvoir réglementaire de rendre obligatoire le recours à un téléservice afin d'accomplir des démarches administratives² ;
- ◆ que toutefois, le pouvoir réglementaire ne peut le faire qu'en garantissant l'accès effectif aux droits, en tenant compte de multiples critères³ : « *Il doit tenir compte de l'objet du service, du degré de complexité des démarches administratives en cause et de leurs conséquences pour les intéressés, des caractéristiques de l'outil numérique mis en œuvre ainsi que de celles du public concerné, notamment, le cas échéant, de ses difficultés dans l'accès aux services en ligne ou dans leur maniement* » ;
- ◆ la garantie d'accès effectif aux droits, en tenant compte des éléments limitant cet accès, peut aller jusqu'à proposer une solution de substitution à l'usage du téléservice mis en œuvre dans le cadre d'une démarche administrative⁴.

¹ CE, 3 juin 2022, n° 452798.

² Considérant 8 : « ni les principes d'égalité devant la loi, d'égalité devant le service public et de continuité du service public, [...], ni le principe de non-discrimination reconnu par l'article 14 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, [...] ne font obstacle, par principe, à ce que soit rendu obligatoire le recours à un téléservice pour accomplir une démarche administrative [...] ».

³ Considérant 9.

⁴ Considérant 10 : « Il [...] incombe [au pouvoir réglementaire], en outre, pour les mêmes motifs, de garantir la possibilité de recourir à une solution de substitution, pour le cas où certains demandeurs se heurteraient, malgré cet accompagnement, à l'impossibilité de recourir au téléservice pour des raisons tenant à la conception de cet outil ou à son mode de fonctionnement ».

Annexe VII

Par conséquent, il convient de prévoir le cas des personnes qui ne pourront s'enrôler dans le système biométrique parce qu'elles sont trop éloignées du système de sécurité sociale (complexité du processus de recueil des gabarits biométriques) ou bien parce qu'elles sont dans l'incapacité de fournir les gabarits biométriques :

- ◆ dans le cas des empreintes digitales, les personnes n'ayant pas ou plus de doigts ou personnes ayant des empreintes digitales détériorées (certains travailleurs manuels) ;
- ◆ dans le cas de la reconnaissance faciale, les personnes défigurées.

Ces personnes ne pourront pas être reconnues par le système biométrique parce qu'elles n'auront jamais fourni, pour un motif légitime, les données permettant de les reconnaître.

Le cas des faux négatifs, c'est-à-dire des personnes régulièrement enrôlées mais non reconnues par le système biométrique, pose des problèmes plus grands encore. En effet, ces personnes ont fourni les données afin que le système puisse les reconnaître, mais celui-ci n'authentifie pas – à tort – leur identité. En d'autres termes, le système biométrique les identifie comme fraudeurs, alors qu'ils en sont des usagers légitimes. Dans ce cas, il convient que ces personnes, afin de pouvoir exercer leurs droits, puissent s'identifier d'une manière alternative.

2.2. Le système alternatif doit présenter des garanties équivalentes

Les personnes pouvant s'abstraire du système biométrique pour des raisons légitimes, la question du système alternatif se pose.

En particulier, si le système alternatif présente moins de garanties en termes de lutte contre la fraude que le système biométrique, alors les gains attendus de ce dernier seront fortement minorés, les fraudeurs se dirigeant vers le système alternatif pour éviter le système biométrique.

Par conséquent, le projet de système biométrique doit être présenté avec un système alternatif présentant des garanties solides afin qu'il n'y ait pas de déport massif sur ce dernier. À défaut, l'efficacité en termes de lutte contre la fraude serait diminuée, ce qui serait préjudiciable à la proportionnalité de la mesure (voir *supra*).

Pièce jointe 1

Avis de la CNIL

La Présidente

**INSPECTION GENERALE DES AFFAIRES
SOCIALES**

IGAS

Madame CAROLE LEPINE

39-43 QUAI ANDRE CITROEN

75739 - PARIS CEDEX 15

Paris, le 13 mars 2023

N/Réf. : MLD/AGN/CR231149

Saisine n°23001970

(à rappeler dans toute correspondance)

Madame l'Inspectrice générale,

Vous avez sollicité la CNIL concernant différents scénarios, adossés à des solutions techniques, destinés à lutter contre la fraude liée à l'usage des cartes Vitale. Cette sollicitation s'inscrit dans le cadre d'une demande de Monsieur le Ministre de la santé et de la prévention et Monsieur le Ministre délégué chargé des comptes publics.

Vos services ont initialement été missionnés afin de réaliser un recensement des travaux déjà conduits ou accomplis pour évaluer la fraude liée à l'usage des cartes Vitale. Ce recensement vise à permettre de déterminer la portée de la fraude, son origine, sa volumétrie, les modes d'organisation associés et son impact financier.

Les scénarios transmis constituent des pistes de réflexion et de travail et non des propositions définitives : des discussions et travaux complémentaires devront avoir lieu afin de déterminer la pertinence de ceux-ci, définir les mesures à prévoir pour garantir les droits et libertés des personnes et préciser leurs modalités de mise en œuvre. Quel que soit le scénario envisagé, il est prévu que le traitement porte :

- soit sur des données sensibles (données biométriques) dont l'utilisation est soumise à un régime juridique particulier ;
- soit sur le numéro d'inscription au répertoire des personnes physiques (NIR), donnée qui a toujours fait l'objet d'une protection particulière.

Suite à l'examen de ces éléments par le collège des commissaires de la CNIL lors de sa séance du 9 mars 2023, je peux vous faire part des observations suivantes.

RÉPUBLIQUE FRANÇAISE

3 Place de Fontenoy, TSA 80715 - 75334 PARIS CEDEX 07 - 01 53 73 22 22 - www.cnil.fr

1

Remarques générales applicables aux différents scénarios

A titre liminaire, nous estimons qu'il convient de distinguer l'identitovigilance, qui consiste à fiabiliser l'identification du patient et des données le concernant collectées dans le cadre de sa prise en charge, de la vérification de l'identité de l'assurée dans le cadre de la prise en charge financière de soins. Si ces deux opérations sont proches, et peuvent parfois se confondre, les finalités sont différentes, les instruments à mobiliser peuvent être distincts.

Par ailleurs, les remarques qui suivent sont formulées alors que la CNIL n'a été destinataire ni d'une évaluation détaillée de la fraude à l'usage ou à l'enrôlement, ni d'une estimation des lacunes précises des dispositifs d'identitovigilance ou de vérification de l'identité des assurés. En l'état des connaissances, il n'est donc pas possible d'apprécier pleinement la nécessité et proportionnalité des scénarios envisagés et ces remarques demeurent générales.

En premier lieu, certaines parties que vous avez auditionnées vous ont fait part de la nécessité de renforcer les dispositifs existants en matière d'identitovigilance. A cet égard, je souhaite attirer votre attention sur le fait que les dispositifs récemment mis en œuvre à cette fin (l'identifiant national de santé et le téléservice lié) visent d'ores et déjà à sécuriser et à fiabiliser l'identification des usagers et le référencement de leurs données de santé. Dans l'hypothèse où la nécessité de compléter les dispositifs actuels était avérée, il conviendra de s'assurer que les scénarios envisagés concernant la carte Vitale permettent effectivement de les renforcer.

En second lieu, je comprends que les scénarios envisagés entendent lutter contre la fraude aussi bien lors de la délivrance de la carte que de son usage. L'utilisation de données biométriques ou du NIR supposera, compte tenu des risques d'atteintes à la vie privée et aux libertés individuelles susceptibles d'en résulter, qu'un motif d'intérêt public important le justifie. L'identification de ce motif d'intérêt public important place votre travail d'évaluation et de quantification de la fraude comme un prérequis essentiel, afin de justifier de la nécessité de mettre en place l'un des scénarios projetés.

Les deux finalités recherchées – lutte contre la fraude (notamment par la vérification de l'identité de l'assuré), et identitovigilance – devront faire l'objet d'une appréciation autonome au regard de chaque scénario. Cette évaluation devra tenir compte de l'équilibre entre le coût de déploiement et les gains escomptés, des risques et limites des dispositifs existants et des modalités pratiques de déploiement de ces scénarios.

Les moyens envisagés pour lutter contre la fraude sociale ne doivent pas porter une atteinte disproportionnée aux droits à la protection de la santé et à la protection sociale.

Il ressort des dispositifs envisagés pour lutter contre la fraude à l'usage que le bénéfice du tiers payant, voire des soins, serait conditionné à la vérification de l'identité de la personne par les professionnels de santé. Toutefois, il semble que, sauf à confier aux professionnels de santé une mission de contrôle de l'identité des personnes, cela ne relève actuellement ni de leurs missions et ni de leurs attributions. Cette vérification pourrait au demeurant être source de confusion avec les procédures de contrôle *a posteriori* prévues par le code de la sécurité sociale.

Pièce jointe 1

Aussi il convient en amont :

- de distinguer dans l'évaluation préalable les effets des dispositifs, d'une part sur la fraude à la délivrance, d'autre part sur la fraude à l'usage, chacune pouvant appeler la mise en œuvre de mesures différentes ;
- d'analyser les effets potentiellement discriminatoires de ces scénarios. La saisine du Défenseur des droits apparaît essentielle afin de compléter l'étude de ces scénarios et leurs impacts sur les droits des personnes ;
- de mener une étude approfondie quant à l'adhésion des professionnels de santé à un tel dispositif, ainsi que des conséquences en matière de prise en charge des personnes et sur le contrat de soins.

Par ailleurs, la création d'un dispositif de vérification de l'identité des assurés sociaux lors des prestations de soins devrait être, du fait de ses enjeux, encadrée par le Parlement, après consultation des parties prenantes (ordres des professionnels de santé, associations de patients et d'usagers, etc.).

Si les discussions parlementaires concluaient à la nécessité de mettre en œuvre un tel dispositif, celui-ci devrait être envisagé dans le cadre d'une expérimentation visant à démontrer la pertinence et l'efficacité de ces mesures, ainsi que l'adhésion des usagers et des professionnels. Cette expérimentation devra conduire à la réalisation d'un bilan qui constituera une condition essentielle afin que le Parlement et la CNIL puissent se prononcer de manière éclairée sur l'éventuelle pérennisation du dispositif.

Dans l'hypothèse où l'un des scénarios devrait être expérimenté, il conviendrait que le cadre juridique prévoit des mesures particulières afin de garantir le respect des droits et libertés des personnes et plus précisément :

- le caractère facultatif de la détention d'une carte Vitale ou d'une carte nationale d'identité (CNI) devra être maintenu ;
- une attention particulière devra être portée aux conditions dans lesquelles la vérification de l'identité de l'assuré social sera réalisée pour le cas des mineurs ;
- la possibilité de déléguer l'usage d'une carte Vitale devra être maintenue, afin de tenir compte des situations particulières de certains assurés sociaux ;
- les personnes concernées devront être clairement informées quant aux conditions de mise en œuvre du dispositif, aux droits dont elles disposent et aux risques qu'il implique en matière de protection de la vie privée ;
- des alternatives au dispositif choisi, indispensables afin de préserver les droits des personnes et garantir une égalité dans la prise en charge de leurs dépenses de santé, devraient être maintenues. Ces alternatives devront, en tout état de cause, présenter des garanties et un niveau de sécurité équivalents aux dispositifs envisagés, afin que leur efficacité ne s'en trouve pas amoindrie. Elles ne devront pas accentuer la fracture numérique, en prévoyant une alternative physique ;
- des mesures de sécurité de haut niveau devront être prévues pour encadrer le dispositif (minimisation des données, chiffrement des échanges, contrôle d'accès, cloisonnement des données et non-conservation des modèles biométriques, politique de prévention et de gestion d'incidents, politique de gestion des habilitations et des accès, etc.) ;

Pièce jointe 1

les professionnels de santé et le personnel des organismes d'assurance maladie obligatoire devront être spécialement formés à l'utilisation de ce dispositif et sensibilisés aux conséquences pour la vie privée des personnes.

Remarques sur les scénarios faisant intervenir la biométrie

Les deux premiers scénarios envisagent de recourir à la biométrie pour vérifier l'identité de la personne lors de la création de la carte Vitale et/ou à chaque utilisation de celle-ci, soit par la constitution d'un fichier centralisé contenant des données biométriques, soit par la conservation des données biométriques de l'assuré sur la puce de sa carte Vitale. Ces scénarios ne précisent pas quelles données biométriques pourraient être utilisées (empreinte digitale, reconnaissance faciale ou autre) ce qui emporte des risques différents.

Dans ces hypothèses, des modes alternatifs de vérification d'identité devront être prévus afin de tenir compte de la nature statistique de la reconnaissance faciale ou digitale, des risques d'erreur de la technologie (faux positif/faux négatif), de l'indisponibilité des dispositifs et des situations particulières de certains assurés (par exemple les personnes se trouvant dans l'impossibilité matérielle, temporaire ou permanente, de recourir à ce type de procédure).

La CNIL s'interroge sur l'articulation de ces scénarios avec la délégation d'usage de la carte Vitale, nécessaire pour répondre aux situations de certains assurés sociaux. Ces pratiques, aujourd'hui loin d'être marginales, ne sont pas prises en compte. De plus, le déploiement pratique de ces scénarios dans les lieux d'exercice des professionnels de santé donne lieu à des questionnements : l'ensemble des professionnels devront être dotés de dispositifs permettant de collecter et traiter des données biométriques et cette collecte devra être réalisée d'une manière compatible avec la prise en charge sanitaire des personnes (règles d'hygiène, rapidité et qualité de la collecte).

Enfin, concernant le recours à un dispositif de reconnaissance faciale dans le cadre de la délivrance de la e-carte Vitale, la CNIL a admis l'utilisation d'un tel dispositif à certaines conditions qui trouveraient également à s'appliquer ici (dispositif facultatif, conservation minimale du gabarit, recours à terme au Service de garantie de l'identité numérique – SGIN-, ...).

Le bilan relatif à l'expérimentation de la e-carte Vitale devrait être prochainement communiqué à la CNIL et ne pourra appuyer la pérennisation du dispositif que s'il démontre les avantages substantiels du recours à la biométrie pour l'enrôlement lors de la création de la e-carte Vitale, ainsi que la fiabilité du dispositif et notamment que les risques de faux positifs ou négatifs sont suffisamment maîtrisés.

Compte tenu à la fois de la sensibilité des données en cause, des conséquences prévisibles pour la prise en charge sanitaire des personnes et des potentiels détournement d'usage de ces traitements, ces scénarios présentent le niveau de risques le plus élevé d'atteintes à la vie privée et aux libertés individuelles. **La CNIL n'est donc pas favorable à leur mise en œuvre, à plus forte raison en l'absence du bilan précité.**

Pièce jointe 1

Par ailleurs, je souhaite vous faire part des remarques que la CNIL a déjà eu l'occasion de formuler s'agissant du traitement de données biométriques :

- la mise en œuvre d'un tel traitement ne peut être admise que dans la mesure où un motif d'intérêt public important le justifie ou si la personne a donné son consentement au traitement de telles données ;
- le recours à des dispositifs d'authentification biométrique pour s'assurer de l'identité d'une personne peut être considéré comme acceptable, dès lors que les données biométriques sont conservées dans un support individuel et non dans une base centralisée ;
- une alternative, ne faisant intervenir aucun traitement biométrique, devrait être offerte aux personnes ;
- des réflexions doivent être menées concernant les situations particulières, notamment s'agissant du recueil de données biométriques des personnes en situation de handicap et des mineurs, ainsi que les conditions d'utilisation de cette technologie pour les personnes se trouvant dans l'impossibilité matérielle, temporaire ou permanente, d'attester de leur identité par ce moyen ;
- la conservation des seuls gabarits biométriques, non de la photographie ou des empreintes de la personne, est à privilégier ;
- la durée de conservation des gabarits devrait être strictement limitée aux objectifs poursuivis ;
- la fiabilité du recours à la biométrie devra être analysée, et il devrait être démontré que les risques de faux positifs ou négatifs sont suffisamment maîtrisés ;
- la mise en œuvre de mesures de sécurité de haut niveau doit être prévue (chiffrement des échanges, contrôle d'accès, cloisonnement des données et de non-conservation des gabarits biométriques, prévention et de gestion d'incidents, une politique de gestion des habilitations et des accès).

Remarques sur les scénarios avec utilisation du NIR

Ces scénarios conduiraient à intégrer le NIR sur la nouvelle carte nationale d'identité électronique (CNIe) ou le titre de séjour de l'assuré. Le NIR des assurés serait conservé soit sur la puce du titre dans un conteneur « assurance maladie », soit sur un 2D-Doc.

Ces scénarios auraient pour conséquence directe de permettre l'utilisation de la CNIe ou du titre de séjour en lieu et place de la carte Vitale. Il semblerait que leur mise en œuvre nécessiterait une évolution des caractéristiques techniques des titres d'identité ou de leurs composants, notamment la puce électronique, ce qui imposerait de remplacer les CNIe déjà délivrées.

La CNIL a développé de longue date une logique de cantonnement du NIR, selon laquelle chaque secteur d'activité doit être dotée d'au moins un identifiant sectoriel adapté. Cette doctrine permet de limiter le risque d'interconnexion lié à l'utilisation de cet identifiant particulièrement signifiant. En outre, la CNIL a toujours porté une attention particulière aux mesures de sécurité techniques et organisationnelles mises en œuvre pour le traitement de cette donnée, afin de garantir qu'elle ne soit pas connue de tous.

Pièce jointe 1

Le scénario visant à intégrer le NIR sur un 2D-doc de la CNIe ou d'un titre de séjour n'apparaît pas apporter un niveau de sécurité suffisant. En effet, dans cette hypothèse, le NIR ne ferait pas l'objet d'une mesure de chiffrement particulière et serait donc lisible facilement, directement sur le titre ou sur n'importe quelle photocopie ou scannérisation de celui-ci dans un écosystème ne relevant pas exclusivement du champ de la sécurité sociale. D'autres formats de cachet électronique visible permettant le chiffrement de cet identifiant pourraient néanmoins être envisagés.

Le scénario visant à intégrer le NIR sur la puce du titre constitue donc la solution la moins intrusive et la moins risquée d'un point de vue technique. Cette solution **nécessiterait, en tout état de cause, la réalisation d'une étude technique, juridique et économique poussée**, qui devra impliquer les mesures décrites ci-dessous :

- assurer le cloisonnement du NIR par rapport aux autres données contenues dans la puce de ces titres et de leurs usages, notamment en chiffrant le conteneur « assurance maladie » de manière spécifique et lisible uniquement par les outils et acteurs de la sphère médicale et médico-sociale. En effet, le règlement (UE) 2019/1157 permet aux Etats membres d'intégrer sur la puce d'un titre d'identité ou de séjour d'autres données que celles nécessaires à la preuve de l'identité du titulaire. Ce même texte impose, néanmoins, que ces autres données soient physiquement ou logiquement séparées des données biométriques ;
- mettre en œuvre des mesures particulières de sécurité pour assurer le cloisonnement du NIR tout au long de la procédure de création et de délivrance du titre afin de ne pas communiquer aux services de mairie et de préfecture cet identifiant, si besoin en ayant recours à un tiers de confiance ;
- prévoir l'application du secret professionnel aux accédants du NIR aux fins de création et de délivrance des titres d'identité destinés à le porter ;
- inscrire au niveau de la loi le droit de tout assuré à s'opposer au traitement du NIR sur son titre d'identité ou de séjour ;
- s'assurer que des alternatives soient maintenues pour qu'un assuré puisse prouver ses droits et bénéficier de la prise en charge par l'assurance maladie. Ces alternatives ne devront pas conduire à une stigmatisation des personnes ne disposant pas de leur titre d'identité ou de limitation quant à l'accès aux soins.

Des réflexions complémentaires devraient être menées afin de tenir compte du caractère non-obligatoire de détention d'une CNIe, de l'absence de titre de séjour pour les personnes étrangères mineures ou encore de la situation particulière des ressortissants des autres pays de l'Union européenne.

Mes services se tiennent à votre disposition pour vous accompagner dans les travaux ultérieurs qui pourraient intervenir sur le sujet.

Je vous prie d'agréer, Madame l'Inspectrice générale, l'expression de mes respectueuses salutations.



Marie-Laure DENIS

Pièce jointe 2

Réponse de la DAJ des ministères sociaux

**Réponses de la DAJ (en bleu) des ministères sociaux au
questionnaire de la mission**

24 mars 2023

1. RECOURS (BASE LÉGALE, CONDITIONS, CONSENTEMENT, OBLIGATION DE DÉTENTION)	2
2. MODALITÉS (FRÉQUENCE, ARCHITECTURE).....	6
3. APPLICATION DU PRINCIPE DE PROPORTIONNALITÉ, EFFET / TIERS PAYANT.	9
4. RISQUES (DISCRIMINATION, SÉCURITÉ/IRRÉVOCABILITÉ).....	13

1. Recours (base légale, conditions, consentement, obligation de détention)

La mise en place d'une carte Vitale biométrique soulève un certain nombre de questions, étant donné que le cadre juridique (pour l'essentiel, le RGPD et son article 9) prévoit un principe d'interdiction de son usage. Toutefois, des exceptions existent, notamment lorsque le « *traitement biométrique est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit [...] de la sécurité sociale et de la protection sociale* » et que « *ce traitement est autorisé par [...] le droit d'un État membre* ».

Questions :

- ◆ quelle est la base légale applicable à la mise en place d'une carte Vitale qui contiendrait des données biométriques ?
 - L'une des bases légales qui autorise la collecte de données sensibles est l'exercice de droits propres en matière de sécurité sociale : dans ce cas il n'est pas vérifié le caractère proportionné du traitement à l'objectif poursuivi (contrairement au cas où la collecte est autorisée pour des motifs d'intérêt public important) : la mise en place d'une carte Vitale biométrique pourrait-elle relever de cette seule base ?

Pour rappel, tout traitement de catégories particulières de données à caractère personnel, au sens de l'article 9 du règlement (UE) 2016/679 du 27 avril 2016 (ci-après « RGPD »), communément appelées « données sensibles » et dont font partie les données biométriques, ne peut intervenir que si les deux conditions cumulatives suivantes sont remplies :

- le traitement est valablement fondé sur une des bases légales prévues à l'article 6 du RGPD : en l'espèce, une mission d'intérêt public (article 6.1.e) RGPD) ;
- une des exceptions mentionnées à l'article 9 du RGPD est applicable au traitement concerné : en l'espèce, l'exécution des obligations et de l'exercice des droits propres au responsable de traitement en matière de sécurité et de protection sociale (article 9.2.b) RGPD).

Un précédent illustre bien la conjonction de ces deux critères de licéité, qui ont été entérinés par la CNIL et le Conseil d'Etat, dans sa fonction consultative, dans le cadre de l'utilisation de la biométrie aux fins de délivrance de l'application e-carte Vitale autorisée par le décret n° 2022-1719 du 28 décembre 2022 relatif aux moyens d'identification électronique interrégimes mentionnés aux articles L. 161-31 et L. 161-33 du code de la sécurité sociale.

En revanche, le principe de proportionnalité, principe général applicable à l'ensemble des caractéristiques et conditions de mise en œuvre de tout traitement (les données, leur durée de conservation, leurs destinataires, leurs modalités d'accès, etc.) doit en tout état de cause être systématiquement respecté.

Il est d'ailleurs également rappelé, sur le point particulier du traitement de données sensibles, à l'article 9.2.b) RGPD : « *le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale, dans la mesure où ce traitement est autorisé par le droit de l'Union, par le droit d'un État membre ou par une convention collective conclue en vertu du droit d'un État membre qui prévoit des garanties appropriées pour les droits fondamentaux et les intérêts de la personne concernée* », cette obligation de garanties appropriées étant applicable aux dispositions légales comme aux conventions concernées.

Pièce jointe 2

- ◆ Quel régime s'applique pour le traitement d'une carte Vitale biométrique (s'agit-il d'un traitement mis en œuvre pour le compte de l'Etat dans le cadre de ses prérogatives de puissance publique au sens de l'article 32 de la loi 1978) ?

Un traitement de données permettant la délivrance d'une carte Vitale biométrique relève en effet de l'article 32 de la loi n° 78-17 du 6 janvier 1978 modifiée (loi « Informatique et Libertés »). Ce point a également été entériné par la CNIL dans son avis sur le décret précité du 28 décembre 2022, cf. délibération n° 2022-097 du 8 septembre 2022 :

« La Commission a été saisie d'un projet de décret relatif aux moyens d'identification électronique interrégimes mentionnés aux articles [L. 161-31](#) et [L. 161-33](#) du code de la sécurité sociale (CSS). Ce projet définit les caractéristiques, les modalités de délivrance, d'utilisation et de désactivation des moyens d'identification électronique des assurés et des professionnels et établissements de santé en application de l'article 2 de l'ordonnance n° 2021-581 et, s'agissant du traitement de données biométriques pour l'authentification des personnes, sur le fondement de l'article 32 de la loi « informatique et libertés ».

A noter que les dispositions législatives du code de la sécurité sociale renvoient en tout état de cause à un décret en Conseil d'Etat, pris après avis de la CNIL, soit le même niveau de norme que celui prévu par l'article 32 de la loi « Informatique et libertés », le soin de fixer les « caractéristiques de ce moyen d'identification électronique [le moyen d'identification électronique interrégimes], ses modalités de délivrance, d'utilisation et de désactivation ainsi que les caractéristiques du système d'opposition » (article L. 161-31 du code de la sécurité sociale). Dans la mesure où ces éléments seront vraisemblablement modifiés par la mise en place d'une carte Vitale biométrique, quelle que soit sa forme exacte, un tel traitement devrait donc être encadré, *a minima* et en tout état de cause, par un décret en Conseil d'Etat pris après avis de la CNIL.

- ◆ Le consentement de l'utilisateur au stockage de données biométrique dans une puce de carte Vitale serait-il obligatoire dès lors que le caractère facultatif de la demande de carte Vitale (carte Vitale, e-carte Vitale ou pas de carte Vitale) et que l'absence de possession de la carte ne fait pas obstacle à l'exercice des droits ?

Par principe, notamment pour des traitements publics, le recueil du consentement des personnes au traitement de leurs données ne constitue pas une obligation, à moins que des dispositions spéciales ne l'imposent (c'est le cas par exemple en matière de dépôt de cookies, les dispositions de l'article 82 de la loi « Informatique et Libertés » imposant le recueil du consentement des personnes concernées préalablement à cette opération) ou que les autres bases légales prévues par l'article 6 du RGPD (intérêt public, obligation légale, etc.) ne puissent valablement fonder sa mise en œuvre, en l'absence de garanties suffisantes.

C'est, en substance, le raisonnement suivi par le Conseil constitutionnel en ce qui concerne le partage des données de santé recueillies dans le cadre de la lutte contre le covid-19 à des organismes assurant l'accompagnement social des personnes concernées, qui a estimé que « s'agissant d'un accompagnement social, qui ne relève donc pas directement de la lutte contre l'épidémie, rien ne justifie que la communication des données à caractère personnel traitées dans le système d'information ne soit pas subordonnée au recueil du consentement des intéressés » et a donc jugé contraires à la Constitution certaines dispositions de la loi du 11 mai 2020 (cf. Décision n° 2020-800 DC du 11 mai 2020, point 70).

Ces deux hypothèses (disposition spéciale imposant le consentement et absence de validité de la base légale « mission d'intérêt public ») ne semblent pas applicables à la délivrance de cartes

Pièce jointe 2

Vitale biométriques, sous réserve qu'il soit démontré que le recours à la biométrie est nécessaire aux fins poursuivies.

Le caractère facultatif de la détention de la carte, de même que son absence d'incidence sur les droits sociaux dont bénéficient les assurés sociaux, ne semble pas davantage impliquer nécessairement le recueil d'un consentement, qui n'est par exemple pas requis pour le traitement des données biométriques nécessaires à la délivrance des passeports et cartes d'identité, titres dont la détention est pour les deux titres facultative.

- ◆ Les données alimentant la carte Vitale sont issues des traitements relatifs aux « référentiels bénéficiaires des organismes d'AMO ». En raison de la mission d'intérêt public dont est investie l'assurance maladie, les droits d'opposition et d'effacement sont écartés pour ces traitements, notamment en application du décret n° 2015-390 du 3 avril 2015. Serait-il possible de s'appuyer sur ce décret pour une carte Vitale biométrique ?

Le traitement biométrique nécessaire à la délivrance d'une carte Vitale biométrique n'est pas couvert par ce décret et devra donc faire l'objet d'un encadrement spécifique.

Si, au strict plan juridique, dès lors que le décret précité de 2015 constitue un décret en Conseil d'Etat pris après avis de la CNIL, cet encadrement pourrait figurer dans ce décret, une telle situation n'apparaît ni opportune ni recommandée d'un point de vue légistique : ce décret couvre déjà de très nombreuses catégories de traitements, qui au demeurant ne relèvent plus de ce niveau de norme depuis l'entrée en vigueur du RGPD, et il apparaît dès lors préférable de prévoir un encadrement *ad hoc* pour la mise en œuvre de la carte Vitale biométrique.

Le fait que les droits d'opposition et d'effacement soient écartés pour certains traitements mis en œuvre aux fins de gestion des régimes d'assurance-maladie est sans incidence sur la proportionnalité d'une telle limitation des droits des personnes à l'égard d'un traitement de données distinct : dans la mesure où le traitement de données nécessaire à la mise en œuvre d'une carte Vitale biométrique constitue un traitement distinct, une telle limitation doit faire l'objet d'un examen autonome, quelle que soit la nature de la mesure juridique encadrant ledit traitement (décret n° 2015-390 du 3 avril 2015 modifié ou décret *ad hoc*). En revanche, le décret encadrant ledit traitement pourrait tout à fait, dès lors que cela est justifié et proportionné, exclure certains droits des personnes, dans des conditions conformes à l'article 23 du RGPD (qui liste les motifs, parmi lesquels un intérêt public dans le domaine de la sécurité sociale – e) du 1. – et prévoit les conditions dans lesquelles les droits des personnes peuvent faire l'objet de limitations).

- ◆ La détention, d'une part, et l'utilisation, d'autre part, d'une carte Vitale peut-elle être rendue obligatoire ? Autrement dit, l'exercice des droits sociaux peut-il être subordonné à l'utilisation de la carte Vitale ou à la présentation d'une carte Vitale ? (aujourd'hui c'est facultatif)

L'ouverture du droit aux prestations de l'assurance maladie n'est pas inconditionnelle et est d'ores et déjà déjà subordonnée à la production de documents (L. 161-33 CSS). Par ailleurs, chaque assuré social « dispose » (art. L. 161-31 CSS) d'une carte Vitale.

Néanmoins, si le législateur souhaitait conditionner l'accès aux soins à la présentation et à l'utilisation de la carte Vitale, il se heurterait très probablement à un obstacle d'ordre constitutionnel : en effet, si le Conseil constitutionnel peut opérer une conciliation entre des objectifs à valeur constitutionnelle, il y a peu de doute sur le fait qu'il ferait prévaloir la protection de la santé sur le bon usage des deniers publics (si l'objectif de la mesure est la prévention de la fraude).

Pièce jointe 2

- ◆ Quel est aujourd'hui le cadre normatif permettant à des professionnels de santé d'opérer un contrôle d'identité ou une vérification d'identité (en établissement de santé, en médecine de ville, officine...) ? Pourrait-on, dans un objectif de lutte contre la fraude, confier aux professionnels de santé/médecine de ville une compétence de vérification de l'identité ? Même question dans un objectif de qualité et de sécurité des soins (identitovigilance) ? Pourrait-on confier, sur la base par exemple d'une disposition législative, à des professionnels de santé, un rôle de face-à-face dans l'enrôlement biométrique des assurés pour l'activation d'une carte Vitale biométrique ?

⇒ Sur le cadre normatif actuel :

Il n'existe pas d'obligation générale pour les professionnels de santé de contrôler l'identité des patients (seules les forces de l'ordre sont aujourd'hui qualifiées pour vérifier, dans les conditions prévues par la loi, les identités). Il existe toutefois dans le droit positif des dispositions explicites imposant à l'assuré social ou au bénéficiaire de la CME de permettre à l'établissement de santé le prenant en charge d'être remboursé (R. 1112-4 et R. 1112-24 du CSP) et ainsi de fournir la justification de ses droits sociaux et, partant, de son identité.

A l'inverse, aucune pièce d'identité ne peut, par exemple, être exigée pour sauvegarder le secret de la grossesse ou de la naissance (R. 1112-28 CSP). Une disposition analogue existe pour les toxicomanes (R. 1112-38)

S'agissant de la médecine de ville, aucune disposition prévoyant une obligation pour le patient de décliner son identité n'a été identifiée.

⇒ Sur une loi qui viendrait imposer la vérification de l'identité des patients au soignant :

S'agissant d'un autre cadre, le Conseil constitutionnel a jugé que : « *Les objectifs de valeur constitutionnelle de prévention des atteintes à l'ordre public et de recherche des auteurs d'infractions peuvent justifier que soient engagées des procédures de contrôle d'identité. S'il est loisible au législateur de prévoir que les contrôles mis en œuvre dans ce cadre peuvent ne pas être liés au comportement de la personne, la pratique de contrôles d'identité généralisés et discrétionnaires serait incompatible avec le respect de la liberté personnelle, en particulier avec la liberté d'aller et de venir.* (2022-1025 QPC, 25 novembre 2022)

Une disposition législative qui imposerait au médecin de vérifier l'identité du patient (sans parler de l'enrôlement du patient) ne semble pas juridiquement admissible.

En revanche, une disposition législative qui compléterait l'article L. 161-31 CSS pour imposer à l'assuré social de justifier auprès du soignant de cette qualité (et donc de son identité) uniquement pour la prise en charge des soins pourrait être envisagée sous néanmoins plusieurs réserves (sans non-exhaustives) :

- Les soins qui laissent la possibilité au patient de demander l'anonymat ;
- La possibilité pour un patient de ne pas faire valoir cette qualité d'assuré social ;
- Les soins urgents ne peuvent être conditionnés à la présentation de la carte Vitale ;
- Les personnes inconscientes, en perte de discernements etc.

De nombreuses incertitudes subsistent sur la réception par le juge notamment constitutionnel de dispositifs dont l'objet viendrait restreindre l'accès aux soins.

Au-delà des réponses précédentes, la DAJ estime que la mise en œuvre d'une carte Vitale biométrique pose en outre la question de la nécessité du recours à la loi pour en autoriser la mise en œuvre.

Pièce jointe 2

En effet, par principe, la mise en œuvre d'un traitement de données relève d'un encadrement réglementaire. Le Conseil d'Etat a en particulier jugé, s'agissant d'un traitement particulièrement sensible et à certains égards similaire à celui qui créerait une carte Vitale biométrique, à savoir le fichier biométrique des demandeurs de passeport et de carte d'identité, que le pouvoir réglementaire était compétent pour en fixer les conditions de mise en œuvre « *sans que puisse avoir d'incidence à cet égard la circonstance que ce traitement a vocation à contenir les données de la quasi-totalité de la population française.* » (Conseil d'Etat, 18 octobre 2018, M. H... G...et association Génération Libre, n° 404996, points 3 et 4).

Néanmoins, on peut observer une tendance forte à l'intervention du législateur sur les questions relatives au traitement de données à caractère personnel, sans que celle-ci soit pour autant nécessaire en application de l'article 34 de la Constitution. Le Conseil d'Etat a lui-même reconnu, s'agissant du même traitement biométrique des demandeurs de passeport et de carte d'identité, qu'il était loisible, compte tenu du sujet, de recourir à la loi :

« 7. S'agissant enfin du niveau hiérarchique de la norme requise, un tel fichier, dès lors qu'il respecterait, dans les conditions qui précèdent, les garanties fondamentales prévues notamment par l'article 6 de la loi du 6 janvier 1978, pourrait être créé par décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés, ainsi que le prévoit l'article 27 de la même loi s'agissant des traitements contenant des données biométriques nécessaires à l'authentification des personnes. Toutefois, compte tenu de l'ampleur du fichier envisagé et de la sensibilité des données qu'il contiendrait, il n'est pas interdit au Gouvernement, s'il le croit opportun, d'emprunter la voie législative. » (Conseil d'Etat, Section de l'intérieur, 23 février 2016, Avis n° 391080)

La question doit en particulier se poser lorsque d'autres libertés fondamentales que la seule protection de la vie privée et de la protection des données à caractère personnel ou que d'autres domaines d'intervention obligatoire du législateur sont en jeu : par exemple, le législateur a dû intervenir dans le champ des enregistrements vidéo, qui constituent des traitements de données, dans la mesure où ils étaient susceptibles d'avoir une incidence sur l'exercice d'autres libertés fondamentales (manifestation, liberté de culte, inviolabilité du domicile).

En l'espèce, il conviendra en particulier de déterminer si la mesure envisagée affecte ou non les principes fondamentaux de la sécurité sociale au sens de l'article 34 de la Constitution pour en déduire le niveau de norme requis pour la mettre en œuvre.

En tout état de cause, une modification de l'article L. 161-31 du code de la sécurité sociale, qui prévoit notamment que le « moyen d'identification interrégimes » que constitue la carte Vitale peut être « *matériel ou immatériel* » (précision apportée par l'ordonnance n° 2021-581 du 12 mai 2021) et « *comporte la photographie de son titulaire* » (précision apportée par la loi n° 2004-810 du 13 août 2004), pourrait s'avérer nécessaire.

2. Modalités (fréquence, architecture)

S'agissant de la carte Vitale biométrique, plusieurs cas de figure sont à distinguer, en ce qui concerne le type de biométrie envisagée ainsi que la nature de l'usage et de l'architecture de la biométrie :

- ◆ un traitement biométrique peut être effectué à l'« enrôlement » uniquement, c'est à dire lors de la demande de création de la carte Vitale dans le système d'information de l'assurance maladie et de l'enregistrement de son bénéficiaire, aucun contrôle de cette nature n'étant ensuite demandé lors de l'usage de la carte Vitale. Autre cas d'utilisation de la biométrie : le recours à un traitement biométrique à chaque présentation de la carte

Pièce jointe 2

Vitale par son porteur pour exercer ses droits en matière d'AMO, c'est à dire de manière systématique (ou quasiment), lors de chaque interaction de l'utilisateur avec le système de santé (chez le médecin / à la pharmacie...);

- ◆ les gabarits biométriques c'est-à-dire les données biométriques qui servent de référence pour authentifier le porteur de la carte peuvent être stockés « localement » et uniquement dans la carte Vitale (« biométrie sur carte ») ou dans une base de données centralisée (architecture permettant, en sus de l'authentification, l'identification d'un gabarit par comparaison de ceux en base) ;
- ◆ la biométrie peut être plus ou moins invasive dans son usage, avec une fiabilité variable selon le type de biométrie mis en œuvre. À ce stade, parmi les nombreux types de biométrie envisageables, la mission n'envisagera que la reconnaissance faciale, la reconnaissance d'empreintes digitales et, si cela est possible, la reconnaissance d'empreinte de l'iris.

La mission s'interroge sur la faisabilité et les conséquences juridiques de ces choix, tant sur la nature du recours (usage/enrôlement) que sur l'architecture choisie, impactant les traitements de données (donnée stockée sur la carte/centralisée en base) : cf. schéma ci-dessous. On voit bien qu'en croisant ces deux éléments, on obtient des scénarios plus ou moins risqués et attentatoires aux libertés (cas A, B, C, D ci-dessous).

-		Fréquence du traitement biométrique (de + à ++++)	
-		A l'enrôlement (lors de la création de la carte)	A chaque utilisation de la carte vitale chez un professionnel de santé
Architecture du traitement biométrique	Le gabarit biométrique est uniquement stocké sur la carte physique sur un mode décentralisé	CAS A (+) Un traitement est opéré à l'enrôlement uniquement ce qui permet d'authentifier que le détenteur de la carte est bien son bénéficiaire.	CAS B (++) Outre le traitement à l'enrôlement, un traitement d'authentification est opéré à chaque passage chez un professionnel de santé pour s'assurer que le porteur de la carte est le bénéficiaire.
	Le gabarit biométrique est stocké dans une base centralisée (éventuellement anonymisée)	CAS C (+++) Outre un traitement d'authentification, un traitement d'identification est opéré une fois à l'enrôlement pour vérifier qu'à une empreinte ne correspond qu'un seul individu	CAS D (++++) Outre le traitement d'identification à l'enrôlement, un traitement d'authentification avec recherche dans la base est opéré à chaque passage chez un professionnel de santé.

Questions :

- ◆ Quelle est la faisabilité juridique d'une carte Vitale biométrique dans l'hypothèse où le traitement biométrique ne serait réalisé qu'à l'enrôlement (cas de l'expérimentation en cours pour l'application e-carte Vitale)? Même question, dans l'hypothèse d'une utilisation à chaque passage chez un professionnel de santé ? Il n'existe en France que deux cas d'utilisation de la biométrie à l'usage : lors du retrait de la CNIe (l'agent de la mairie doit vérifier que la carte délivrée est bien délivrée à son porteur légal par l'apposition des empreintes) et lors du passage dans les sas PARAFE aux aéroports.

Il n'existe pas d'interdiction juridique de principe, pour aucune de ces deux catégories d'usage (biométrie à l'enrôlement, biométrie « à l'usage »).

Ces deux scénarios sont dès lors juridiquement envisageables dès lors que les conditions de légalité des atteintes au droit à la protection des données sont satisfaites : en synthèse, celles-

Pièce jointe 2

ci doivent être justifiées par un motif d'intérêt général et être adéquates et proportionnées à cet objectif.

Il n'est dès lors pas possible de répondre plus précisément sur la faisabilité juridique de chacun de ces scénarios en l'absence de détails sur les objectifs précisément poursuivis par chacun d'eux, non pas en termes de fonctionnalités mais sur la nature et l'étendue des intérêts poursuivis. Seule la détermination exacte de ces objectifs permet, d'une part, de mesurer l'intensité des atteintes à la vie privée et à la protection des données qu'ils sont susceptibles de justifier et, d'autre part, de déterminer les conditions adéquates et proportionnées de mise en œuvre des mesures projetées.

A titre d'illustration, il est établi que la lutte contre la fraude sociale est un objectif à valeur constitutionnelle, susceptible de justifier des ingérences dans les droits fondamentaux (cf. par exemple Conseil Constitutionnel, Décision n° 2019-789 QPC du 14 juin 2019). Il convient néanmoins de qualifier précisément la nature de cette fraude afin de déterminer les mesures de lutte qui peuvent être légalement être mises en œuvre : à titre d'illustration, si la fraude constatée (ou présumée sur la base d'indices concordants) ne concerne pas l'usage, les cas B et D seront manifestement disproportionnés.

Il en est de même pour les autres objectifs susceptibles d'être poursuivis, y compris en matière d'identité-vigilance : c'est à l'aune de leur définition précise que la légalité des dispositifs peut être examinée.

En revanche, la DAJ confirme les analyses de l'IGAS sur le caractère plus ou moins attentatoire des cas d'usage identifiés : cette grille de lecture est par exemple celle suivie par la CNIL, qui distingue la conservation sur support individuel et la conservation en base ; en outre, l'augmentation de la fréquence des traitements biométriques opérés augmente mécaniquement les risques de faux positifs et faux négatifs que le système, pour être proportionné, doit maîtriser. Au titre des critères de sensibilité du dispositif, on peut ajouter également la nature de la biométrie en cause, certaines technologies biométriques faisant peser par elles-mêmes des risques plus importants pour les droits des personnes (reconnaissance faciale en particulier).

- ◆ Le cadre juridique actuel permettrait-il d'effectuer des traitements d'authentification et des traitements d'identification du porteur de la carte, dans un objectif de lutte contre la fraude ? Il n'existe pas en France de traitement biométrique d'identification, en dehors des cas prévus dans le cadre d'affaires de police judiciaire.

Le cadre constitutionnel et conventionnel n'interdit pas de mettre en œuvre des traitements, y compris biométriques, aux fins de lutte contre la fraude, y compris sociale, qui constitue un objectif à valeur constitutionnel. Dans le champ des traitements de données dans le domaine de la sécurité sociale, le Conseil constitutionnel a ainsi indiqué, dans sa décision n° 2004-504 DC, que l'équilibre financier de l'assurance maladie était une exigence constitutionnelle. De nombreuses dispositions légales se fondent d'ailleurs sur un objectif de lutte contre la fraude (en matière fiscale, sociale, etc.), y compris des dispositions législatives prévoyant la mise en œuvre de traitements de données biométriques notamment à des fins de lutte contre la fraude en matière d'entrée et de séjour des étrangers (cf. article L. 142-1 du code de l'entrée et du séjour des étrangers et du droit d'asile).

En revanche, comme pour tout autre objectif d'intérêt général, des conditions adéquates et proportionnées au but poursuivi doivent être prévues pour la mise en œuvre de tels traitements de données. Les garanties mises en œuvre doivent être d'autant plus fortes que, comme en l'espèce avec le traitement de données sensibles, ces traitements sont fortement attentatoires au droit à la protection des données.

Pièce jointe 2

- ◆ La seule base de données biométriques où sont stockées les empreintes de la population est le fichier TES, quels seraient les obstacles juridiques à la réutilisation des empreintes digitales contenues dans le fichier TES pour effectuer le traitement de l'enrôlement de la carte Vitale biométrique ?

Deux obstacles juridiques peuvent être mentionnés :

- du point de vue formel : dans la mesure où cette utilisation n'est pas prévue par le décret n° 2016-1460 du 28 octobre 2016 modifié autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité, ce décret en Conseil d'Etat devrait être modifié, après avis de la CNL, afin de compléter les finalités du fichier TES et les destinataires des données qu'il comporte ;

- sur le fond : cette réutilisation de données constituant un traitement à part entière (un « traitement ultérieur » au sens des articles 5.1.b) et 6.4 du RGPD), cette réutilisation serait également examinée, par la CNIL comme par le Conseil d'Etat dans sa fonction consultative, sous l'angle de sa nécessité et de sa proportionnalité. En outre, cela nécessiterait de justifier de la compatibilité de la finalité de la réutilisation des données biométriques du fichier (l'enrôlement de la carte Vitale biométrique) avec les finalités du fichier TES telles que définies dans le décret n° 2016-1460 précité (procéder à l'établissement, à la délivrance, au renouvellement et à l'invalidation des cartes nationales d'identité et des passeports ; prévenir et détecter leur falsification et contrefaçon ; lutter contre l'usurpation d'identité), le RGPD établissant que les données doivent être collectées « *pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités* » (art. 5.1.b) RGPD) et listant les critères d'appréciation de cette compatibilité (art. 6.4 RGPD, qui cite, parmi ces critères, la nature des données en cause : en présence de données biométriques, par exemple, la compatibilité est plus difficile à établir).

3. Application du principe de proportionnalité, effet / tiers payant

Par ailleurs, la question du traitement du cas de l'assuré social n'étant pas reconnu par le dispositif biométrique (quelle qu'en soit la raison) appelle une attention particulière, notamment s'il existe des moyens de contournement du dispositif. En particulier, s'agissant de la carte Vitale, la conséquence de la non-identification d'un assuré social se limite à l'obligation de transmettre une feuille de soins papiers (entraînant des frais pour sa remise et des délais allongés pour le remboursement), l'assuré étant remboursé *a posteriori*. Il apparaît toutefois, pour l'assurance maladie obligatoire, que le tiers payant est obligatoirement accordé aux assurés suivants¹ :

- ◆ en cas de maternité (article L. 160-9 du CSS, dernier alinéa) ;
- ◆ en cas d'accident du travail ou de maladie professionnelle (CSS, art. L. 432-1) pour les soins assurés par les praticiens et auxiliaires médicaux, à l'exception des transporteurs sanitaires ;
- ◆ en cas d'hospitalisation, sous certaines conditions (CSS, art. L. 162-21-1) ;
- ◆ pour les bénéficiaires de la complémentaire santé solidaire (CSS, art. L. 861-1), sous certaines conditions de ressources ;
- ◆ pour les assurés sociaux atteints d'une affection de longue durée exonérante (CSS, art. D. 160-4). De manière générale, l'article L. 16014 du CSS prévoit un grand nombre de cas de dispense ou de limitation de la participation de l'assuré ;

¹ Les ressortissants de l'AME, qui bénéficient également du tiers payant obligatoire (CSS, art. L. 251-2), ne sont pas des assurés sociaux français.

Pièce jointe 2

- ◆ divers actes particuliers : examen bucco-dentaire de prévention (CSS, art. L. 161-1-12) ; consultation de prévention pour les 16-25 ans (CSS, art. L. 161-1-18) ; consultation et analyses biologiques liée à la prescription de contraceptifs pour les assurées de moins de 26 ans (CSS, art. L. 161-4-5)

Questions :

- ◆ Est-il possible de subordonner l'exercice d'un droit social (le tiers payant, instauré à un niveau législatif) à l'authentification de l'identité opérée de manière automatique (exemple : présentation de la carte Vitale) ? et sur la base d'un traitement biométrique (exemple : authentification positive par le dispositif biométrique) ?

L'ouverture du droit aux prestations de l'assurance maladie n'est pas inconditionnelle et est d'ores et déjà subordonnée à la production de documents (L. 161-33 CSS). Par ailleurs, chaque assuré social « dispose » (art. L. 161-31 CSS) d'une carte Vitale.

Néanmoins, si le législateur souhaitait conditionner l'accès aux soins à la présentation et à l'utilisation de la carte Vitale, il se heurterait très probablement à un obstacle d'ordre constitutionnel : en effet, si le Conseil constitutionnel peut opérer une conciliation entre des objectifs à valeur constitutionnelle, il y a peu de doute sur le fait qu'il ferait prévaloir la protection de la santé sur le bon usage des deniers publics (si l'objectif de la mesure est la prévention de la fraude).

Il convient par ailleurs de rappeler que l'article 47 de la loi « Informatique et Libertés », reprenant et complétant les dispositions de l'article 22 du RGPD, exclut toute décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative prise sur le seul fondement d'un traitement automatisé de données à caractère personnel. Si ces dispositions prévoient des exceptions à cette interdiction, la mise en œuvre d'un traitement biométrique ne peut bénéficier de l'une d'entre elles, le 2^o dudit article excluant en tout état de cause les décisions administratives individuelles fondées exclusivement sur un traitement portant sur des données sensibles telles que des données biométriques.

- ◆ sur l'analyse du principe de proportionnalité :
 - Dans l'hypothèse de la mise en place d'une carte Vitale comprenant des données biométriques, et en tenant compte du caractère massif (presque la totalité de la population assurée sociale française) du recueil de gabarits biométriques, comment la jurisprudence (constitutionnelle, administrative) apprécie la proportionnalité des traitements au regard des différentes finalités de lutte contre la fraude ?

En matière de lutte contre la fraude comme de tout autre objectif d'intérêt général, les conditions de proportionnalité sont liées à :

- la délimitation des objectifs poursuivis et l'absence de réutilisation ultérieure à d'autres fins ;
- la limitation des données traitées au strict nécessaire compte tenu de cet objectif ; en matière de traitements biométriques, la conservation des seuls gabarits apparaît à cet égard plus conforme au principe de minimisation des données ;
- la durée et les modalités de conservation des données, la première ne devant pas excéder celle nécessaire à l'atteinte de l'objectif poursuivi et les secondes devant être adaptées à ce dernier (support individuel ou base de données) ;
- les destinataires des données traitées, qui doivent être limités à ceux qui concourent aux finalités poursuivies, et leurs conditions d'accès, assorties des garanties organisationnelles et techniques assurant la limitation des accès au strict nécessaire ;

Pièce jointe 2

- les droits des personnes à l'égard du traitement de leurs données, notamment les droits d'opposition et d'effacement, ainsi que le droit de ne pas faire l'objet d'une décision entièrement automatisée ; une alternative doit également être prévue pour les personnes ne pouvant utiliser de traitements biométriques ;

- les mesures de sécurité encadrant la mise en œuvre du traitement.

Les mêmes catégories de garanties sont examinées par tous les ordres de juridiction et le même contrôle est également assuré ex-ante par la CNIL.

S'agissant d'un traitement biométrique mis en œuvre à des fins de lutte contre la fraude, on peut en particulier mentionner l'avis précité du Conseil d'Etat sur le projet TES : *« C'est pourquoi il convient de s'assurer, d'une part, que le recueil et la conservation des données biométriques ne seraient pas disproportionnées au regard des finalités du fichier, d'autre part, que l'accès à ces données et l'usage qui pourrait en être fait s'effectueraient selon des modalités strictement définies garantissant qu'elles ne puissent être utilisées à d'autres fins. »*

Le Conseil constitutionnel s'est quant à lui prononcé sur la carte Vitale électronique dans sa décision n° 99-416 DC du 23 juillet 1999 et a mis en avant les garanties suivantes au soutien de la constitutionnalité des dispositions examinées :

« 46. Considérant qu'aux termes du I de l'article L. 161-31 du code de la sécurité sociale, la carte électronique individuelle « doit permettre d'exprimer de manière précise l'accord du titulaire ou de son représentant légal pour faire apparaître les éléments nécessaires non seulement à la coordination des soins mais aussi à un suivi sanitaire » ; que le II du même article dispose : « Dans l'intérêt de la santé du patient, cette carte comporte un volet de santé... destiné à ne recevoir que les informations nécessaires aux interventions urgentes ainsi que les éléments permettant la continuité et la coordination des soins » ; qu'en vertu du I de l'article L.162-1-6 du code de la sécurité sociale, l'inscription, sur la carte, de ces informations est subordonnée dans tous les cas à l'accord du titulaire ou, s'agissant d'un mineur ou d'un majeur incapable, de son représentant légal ; que les personnes habilitées à donner cet accord peuvent, par ailleurs, « conditionner l'accès à une partie des informations contenues dans le volet de santé à l'utilisation d'un code secret qu'elles auront-elles-mêmes établi » ; que l'intéressé a accès au contenu du volet de santé par l'intermédiaire d'un professionnel de santé habilité ; qu'il dispose du droit de rectification, du droit d'obtenir la suppression de certaines mentions et du droit de s'opposer à ce que, en cas de modification du contenu du volet de santé, certaines informations soient mentionnées ; qu'en outre, il appartiendra à un décret en Conseil d'État, pris après avis public et motivé du Conseil national de l'Ordre des médecins et de la Commission nationale de l'informatique et des libertés, de fixer la nature des informations portées sur le volet de santé, les modalités d'identification des professionnels ayant inscrit des informations sur ce volet, ainsi que les conditions dans lesquelles, en fonction des types d'information, les professionnels de santé seront habilités à consulter, inscrire ou effacer les informations ; que la méconnaissance des règles permettant la communication d'informations figurant sur le volet de santé, ainsi que celle des règles relatives à la modification des informations, seront réprimées dans les conditions prévues par le VI de l'article L. 162-1-6 du code de la sécurité sociale ; que les sanctions pénales prévues par ces dernières dispositions s'appliqueront sans préjudice des dispositions de la section V du chapitre VI du titre II du livre deuxième du code pénal intitulée « Des atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques » ; qu'enfin, le législateur n'a pas entendu déroger aux dispositions de l'article 21 de la loi du 6 janvier 1978 susvisée relatives aux pouvoirs de surveillance et de contrôle de la Commission nationale de l'informatique et des libertés ;

47. Considérant que l'ensemble des garanties dont est assortie la mise en œuvre des dispositions de l'article 36 de la loi, au nombre desquelles il convient de ranger les caractéristiques assurant la sécurité du système, sont de nature à sauvegarder le respect de la vie privée ; »

Pièce jointe 2

Pour une conclusion inverse, on peut rappeler la décision n° 2012-652 DC du 22 mars 2012, dans laquelle le Conseil constitutionnel a censuré les dispositions de la loi relative à la protection de l'identité visant à sécuriser la délivrance de titres biométriques et d'améliorer l'efficacité de la lutte contre la fraude :

« 10. Considérant, toutefois, que, compte tenu de son objet, ce traitement de données à caractère personnel est destiné à recueillir les données relatives à la quasi-totalité de la population de nationalité française ; que les données biométriques enregistrées dans ce fichier, notamment les empreintes digitales, étant par elles-mêmes susceptibles d'être rapprochées de traces physiques laissées involontairement par la personne ou collectées à son insu, sont particulièrement sensibles ; que les caractéristiques techniques de ce fichier définies par les dispositions contestées permettent son interrogation à d'autres fins que la vérification de l'identité d'une personne ; que les dispositions de la loi déferée autorisent la consultation ou l'interrogation de ce fichier non seulement aux fins de délivrance ou de renouvellement des titres d'identité et de voyage et de vérification de l'identité du possesseur d'un tel titre, mais également à d'autres fins de police administrative ou judiciaire ;

11. Considérant qu'il résulte de ce qui précède qu'eu égard à la nature des données enregistrées, à l'ampleur de ce traitement, à ses caractéristiques techniques et aux conditions de sa consultation, les dispositions de l'article 5 portent au droit au respect de la vie privée une atteinte qui ne peut être regardée comme proportionnée au but poursuivi ; que, par suite, les articles 5 et 10 de la loi doivent être déclarés contraires à la Constitution ; qu'il en va de même, par voie de conséquence, du troisième alinéa de l'article 6, de l'article 7 et de la seconde phrase de l'article 8 ; ».

- ◆ Peut-on considérer le principe de proportionnalité comme respecté si pour lutter contre la fraude à l'assurance maladie :
 - il est mis en place un traitement biométrique potentiellement obligatoire et systématique à l'usage des assurés sociaux ?
 - il est mis en place des croisements de fichiers avec les fichiers de l'assurance maladie et du GIE SESAM Vitale ?

Ces deux séries de conditions entrent en ligne de compte dans l'examen du respect des principes de nécessité et de proportionnalité mais n'appellent pas de réponse univoque : le fichier TES pourrait être considéré comme obligatoire dès lors que la détention de l'un des deux titres concernés (carte d'identité et passeport) est nécessaire dans de très nombreuses situations (il concerne ainsi environ 60 millions de personnes) mais a été jugé proportionné par le Conseil d'Etat. De même, de nombreux croisements de fichiers sont mis en œuvre de manière licite, notamment à des fins de lutte contre la fraude.

- ◆ un traitement de comparaison (à l'enrôlement) entre les empreintes déposées et une base (éventuellement anonymisée) des empreintes pour vérifier qu'une telle empreinte n'existe pas préalablement à la demande pourrait-il être considéré comme proportionné eu égard au risque de fraude ?

Comme tout traitement de données, le principe de proportionnalité implique un examen au cas d'espèce et ne saurait interdire par nature une fonctionnalité particulière.

En l'espèce, il implique de qualifier précisément le risque de fraude afin de vérifier si une telle comparaison est adéquate et proportionnée. Indéniablement, « l'anonymisation » ou le caractère non-nominatif de la comparaison (il ne s'agit par définition pas de données anonymes) constitue une condition de mise en œuvre moins attentatoire qu'une identification biométrique nominative. La détermination précise des conséquences tirées de cette comparaison est également nécessaire pour s'assurer de son caractère proportionné.

Pièce jointe 2

- ◆ un traitement de comparaison du gabarit stocké sur la carte avec les empreintes du porteur, à chaque recours / demande d'accès aux soins pourrait-il être considéré comme proportionné eu égard au risque de fraude ?

Tout comme pour les questions précédentes, il est nécessaire que les types de fraude soient précisément caractérisés pour s'assurer qu'un tel usage permet de lutter efficacement contre les fraudes en cause et est dès lors adapté et proportionné.

Néanmoins, la comparaison dite « à la main de l'utilisateur » est considérée par la doctrine en matière de protection des données comme moins attentatoire que la comparaison en base centrale, comme le montrent par exemple les délibérations de la CNIL en la matière².

4. Risques (discrimination, sécurité/irrévocabilité)

La technologie biométrique est également intrinsèquement porteuse d'un risque de discrimination : comme le relèvent aussi bien le Défenseur des droits que la CNIL en 2020 (cf. « technologies biométriques : l'impératif respect des droits fondamentaux », défenseur des droits, 2021). En effet, en soi, les données physiologiques ne sont pas biométriques : elles le deviennent à la suite d'un traitement biométrique, qui repose sur l'exécution d'un algorithme, qui peut comporter, dès sa conception, des biais discriminatoires qui peuvent générer des erreurs d'allocation ou de sélection. C'est ainsi, par exemple, que les algorithmes de reconnaissance faciale sont moins « efficaces » sur les personnes de couleur, la reconnaissance par empreintes digitales sur les femmes, etc.

En outre, la biométrie faisant appel à des caractéristiques du « vivant », les données biométriques sont susceptibles d'évoluer (vieillesse, traumatisme, handicap...), ce qui entraîne des taux de rejet (faux positif et négatif), plus ou moins importants en fonction de la perméabilité de l'algorithme (et du paramétrage du système d'information mettant en œuvre la biométrie).

Questions :

- ◆ Dès lors qu'il existe un biais discriminatoire des technologies biométriques (faux positifs et faux négatifs), est-ce que la « réalisation des démarches administratives dématérialisées doit demeurer une possibilité ouverte à l'utilisateur et non devenir une obligation » (position du Défenseur des droits) ? La question se pose de la même façon pour garantir l'accessibilité aux personnes handicapées, personnes majeures sous tutelle, illettrisme, etc.

Le Conseil d'Etat a récemment affiné sa jurisprudence sur la dématérialisation des démarches administratives. En substance, il considère qu'il est possible de procéder, par voie réglementaire, à la dématérialisation de tout ou partie des démarches administratives des usagers. Toutefois, l'obligation de recourir à un téléservice ne peut être imposée que si l'accès normal des usagers au service public et l'exercice effectif de leurs droits sont garantis. Pour cela, l'administration doit tenir compte de la nature de la démarche qui est dématérialisée, et de son degré de complexité, des caractéristiques de l'outil numérique proposé, ainsi que de celles du public concerné – notamment des difficultés d'accès ou d'utilisation des services en ligne.

² Cf. par exemple Délibération n° 2019-001 du 10 janvier 2019 portant règlement type relatif à la mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail

Pièce jointe 2

Il a ainsi estimé que, pour certaines démarches particulièrement complexes et sensibles, le texte qui impose l'usage obligatoire d'un téléservice doit prévoir une solution de substitution. Il a jugé que tel est le cas, par exemple, pour les demandes de titres de séjour (Conseil d'Etat, Section, Décision n° 452798 du 3 juin 2022). En l'espèce, le Conseil d'État a fixé deux conditions pour que l'obligation d'utiliser un téléservice pour les demandes de titres de séjour soit légale : les usagers qui ne disposent pas d'un accès aux outils numériques, ou qui rencontrent des difficultés dans leur utilisation de l'outil, doivent pouvoir être accompagnés ; s'il apparaît que certains usagers sont dans l'impossibilité, malgré cet accompagnement, de recourir au téléservice, pour des raisons tenant à sa conception ou à son mode de fonctionnement, l'administration doit leur garantir une solution de substitution.

En ce qui concerne spécifiquement les traitements de données biométriques mis en œuvre pour le compte de l'Etat, il est de doctrine constante de la CNIL qu'une alternative non biométrique doit rester ouverte aux personnes qui ne peuvent faire l'objet d'un enrôlement biométrique, notamment s'agissant des personnes en situation de handicap, des mineurs et personnes âgées dont les empreintes digitales sont réputées moins fiables ou pérennes, ou de toute autre personne dans l'impossibilité de recourir à un dispositif biométrique particulier. De nombreux textes réglementaires portent la trace de telles mesures (cf., par exemple, l'article R. 142-2 du CESEDA qui prévoit, s'agissant du traitement VISABIO, que l'impossibilité de collecte totale ou partielle des empreintes digitales est mentionnée dans le traitement). Par ailleurs, tout traitement biométrique repose sur des estimations statistiques de correspondance entre les éléments comparés et comporte dès lors des « faux positifs » (une personne est reconnue à tort) et des « faux négatifs » (le dispositif ne reconnaît pas une personne qui devrait l'être). Selon la qualité et le paramétrage du dispositif, les taux de faux positifs et de faux négatifs peuvent varier, ce qui peut avoir des conséquences très importantes pour les personnes mal reconnues par le dispositif.

L'ensemble de ces points a par ailleurs été examiné par la CNIL dans son avis précité sur la e-carte Vitale ; le décret finalement adopté prévoit d'ailleurs : « *Les assurés peuvent solliciter l'accompagnement de leur organisme d'assurance maladie pour l'installation de l'application carte Vitale.* » (III de l'article R. 161-33-13 du code de la sécurité sociale).

- ◆ Dès lors qu'il existe un risque de fuite de données (même minime), que les données biométriques, en cas de compromission, ne sont pas révocables, dans quelle mesure et jusqu'où la responsabilité de l'Etat ou de l'assurance maladie pourrait-elle être engagée ?

Du point de vue de la protection des données, la responsabilité de l'Etat et des caisses ne peut être engagée qu'en cas de manquement effectif à l'obligation de sécurité qui pèse sur tout responsable de traitement en application de l'article 32 du RGPD : ce n'est pas du fait de la nature des données traitées mais de leurs conditions effectives de traitement que cette responsabilité naît.

L'Etat ne peut pas faire l'objet de sanctions pécuniaires de la part de la CNIL (cf. art. 20 à 22 de la loi n° 78-17) ; des actions de groupe, y compris en réparation, peuvent en revanche être exercées devant la juridiction administrative en cas de manquement aux dispositions du RGPD, notamment en matière de sécurité, dans les conditions prévues à l'article 37 de la loi « Informatique et Libertés ».

ANNEXE VIII

Parangonnage international

SOMMAIRE

1. LE MODÈLE DU PORTUGAL.....	1
2. LES RÉPONSES DU RÉSEAU DES CONSEILLERS AUX AFFAIRES SOCIALES.....	5
2.1. Le Danemark.....	5
2.2. L'Espagne.....	11
2.3. La Suède.....	12
2.4. Les Etats-Unis d'Amérique.....	13

Annexe VIII

Lors de la phase de cadrage de la mission, il est apparu que plusieurs pays européens ou internationaux utilisent la technologie biométrique à des fins d'authentification et/ou d'identification de leurs ressortissants, notamment pour l'émission de titres d'identité régaliens (cf. annexe XX).

La mission a interrogé le réseau des conseillers pour les affaires sociales (CAS) de la direction des affaires européennes et internationales (DAEI) pour déterminer s'il existe des dispositifs similaires à celui de la carte Vitale projetés ou mis en œuvre dans d'autres pays, et, si tel est le cas, quelles sont les mesures prises visant à sécuriser l'utilisation des cartes d'assurance maladie nationales (lorsqu'elles existent), ainsi que la technologie utilisée (facteur biométrique ou non).

Par ailleurs, le cas du Portugal est apparu comme étant intéressant à investiguer en particulier, puisqu'il permet, comme le système français, d'identifier les assurés sociaux par un numéro de sécurité sociale spécifique, mais, contrairement au système français, la carte qui en est le support est la carte nationale d'identité électronique sécurisée, embarquant (pour la partie « identité » uniquement) des données biométriques. En l'absence de conseiller social, la mission a sollicité l'Ambassade du Portugal afin d'obtenir des informations complémentaires sur le modèle portugais.

Cette annexe présente successivement :

- ◆ les réponses de l'Ambassade du Portugal aux questions de la mission ;
- ◆ les réponses du réseau des CAS au questionnaire de la mission transmis au réseau des CAS.

1. Le modèle du Portugal

Les réponses au questionnaire ci-dessous ont été établies par l'Agence de Modernisation Administrative portugaise (AMA, Administrative Modernisation Agency), en lien avec l'Ambassade du Portugal.

1. **La carte nationale d'identité, qui contient le numéro de sécurité sociale, est-elle le support des droits ouverts à l'assurance maladie obligatoire, permettant à l'assuré la prise en charge et le remboursement des frais de santé ? Permet-elle d'accéder à d'autres données (espace santé, dossier médical...) ?**

Réponse : La carte d'identité nationale au Portugal, Cartão de Cidadão, contient le numéro de sécurité sociale et le numéro d'utilisateur de la santé, le premier étant utilisé pour l'identification et l'accès aux services de sécurité sociale et le second pour l'accès aux services de santé publique (e.g hôpitaux, centres de santé, postes médicaux).

L'accès à d'autres services, notamment électroniques, s'effectue souvent à l'aide du composant électronique du document (chip/puce) avec authentification par un certificat d'authentification, ou à l'aide de services tels que la Mobile Digital Key (ID mobile) pour l'authentification sur les plateformes électroniques.

Pour plus de précisions, la loi qui régit ces questions est la loi n° 7/2007, du 5 février.

2. **Décrire son/ses format(s) : support physique, support dématérialisé (application sur téléphone mobile...) ?**

Réponse :

La carte de citoyen, Cartão de Cidadão, fournit électroniquement toutes les informations également disponibles dans le document physique, en ajoutant des certificats électroniques d'authentification et de signature qualifiée (QDS), permettant au citoyen de s'authentifier auprès de services informatisés, à distance ou localement.

Annexe VIII

La clé mobile numérique (ID mobile) est un service dématérialisé qui peut être utilisé sur n'importe quel système d'Information électronique, à condition qu'elle soit préalablement intégrée à ce service fourni par l'État portugais. C'est un prestataire d'authentification dématérialisé qui certifie l'identité du Citoyen.

Encadré 1 : Chave Móvel Digital (Digital Mobile Key)

Mobile Identification - The Digital Mobile Key is a secure mobile authentication and signature mechanism associated with the Citizen Card and other documents, through the introduction of a username (citizen's mobile number), password (chosen by the citizen) and a one-time password sent by SMS, e-mail or Twitter account (also chosen by the citizen). The eID scheme concerning the Digital Mobile Key was published in OJEU 2020/C 116/01 with a 'high' Level of Assurance. Established by Law No. 37/2014, of 26 June 2014 and Law No. 32/2017, of 26 June 2017, added eSignature features. Administrative Rule No. 73/2018 defines the terms and conditions for use of the SCAP (Professional Attributes Certification System) for the certification of professional, business and public attributes through the Citizen Card and the Digital Mobile Key.

Source : Ambassade du Portugal en France ; Agence de Modernisation Administrative portugaise.

ID.GOV.PT est la nouvelle génération d'identification, utilisant un concept dématérialisé de portefeuille documentaire, multi-documents, permettant l'identification et l'authentification par lecture visuelle directe et dématérialisée (QR Code).

Encadré 2 : ID.gov.pt

The ID.gov.pt app is a digital wallet available for iOS and Android that allows citizens to view, save and share certified versions of personal identification documents, including the national ID card (Citizen Card), the driver's licence and the vehicle registration document, among others. The digital documents generated by the app, which requires secure authentication via the eIDAS-compliant Digital Mobile Key, have the same legal value as the original paper versions, and can be validated by public and private authorities in real-time through a QR code available in the application or through the insertion of a temporary code in a reserved area of Autenticacao.gov.pt. ID.gov.pt is legally supported by Law No. 37/2014^o, of 26 June 2014, amended by Article 407 of Law No. 2/2020, which guarantees citizens the portability of their personal data (in compliance with the GDPR).

Source : Ambassade du Portugal en France ; Agence de Modernisation Administrative portugaise.

En résumé, le titulaire d'une carte de citoyen en cours de validité peut, s'il le souhaite et après authentification sécurisée, obtenir une version numérique de sa carte de citoyen dans l'application mobile, conformément à l'article 4a de la loi n° 37/2014, du 26 juin.

3. Quelles sont les données qui figurent sur la puce de la carte ?

Réponse : Les données contenues dans la composante électronique du document sont :

- ◆ nom ;
- ◆ nom de famille ;
- ◆ numéro de document (comprend le numéro d'identification civile) ;
- ◆ genre ;
- ◆ taille ;
- ◆ nationalité ;
- ◆ date de naissance ;
- ◆ affiliation (nom de la mère, nom du père) ;
- ◆ numéro d'identification fiscale ;
- ◆ numéro de sécurité sociale ;
- ◆ numéro d'utilisateur de santé ;
- ◆ ménage ;

Annexe VIII

- ◆ certificat d'authentification électronique ;
 - ◆ certificat électronique de signature qualifiée.
4. **Des données biométriques figurent-elles sur la carte (physique ou dématérialisée) ou une technologie biométrique est-elle utilisée pour authentifier le patient ?**

Réponse : Oui, il contient des données biométriques qui peuvent être utilisées dans l'authentification Citizen.

La fonctionnalité de lecture ou tout autre traitement des empreintes digitales contenues dans le circuit intégré de la carte de citoyen peut être utilisée à la demande de son titulaire, afin de respecter les principes de la protection des données (cf. actuellement article 14, paragraphe 4 de la loi n° 7/2007 du 5 février)

- **Si oui, la technologie biométrique est-elle utilisée à l'enrôlement (c'est-à-dire lors de la première demande de carte par le bénéficiaire, lors de la création de la carte), ou à l'usage, c'est-à-dire à chaque visite chez le professionnel de santé / à chaque passage en établissement de santé ?**

Réponse : Quand le document est demandé et quand il est collecté et activé. Vous pouvez également être invité à déverrouiller les broches associées au document.

- **Les données biométriques sont-elles présentes sur la carte et sont-elles également stockées dans un fichier centralisé ?**

Réponse : Oui.

- **Si les données biométriques ne sont pas stockées dans un fichier centralisé : comment est-il procédé à un traitement d'identification pour s'assurer de l'unicité de l'empreinte biométrique parmi l'ensemble de la population demandant une carte d'identité ? Autrement dit, comment s'assure-t-on qu'un individu (disposant d'une seule empreinte biométrique) ne puisse pas posséder plusieurs cartes d'identité ?**
5. **Existe-t-il des fraudes spécifiquement liées à l'utilisation de cette carte (usurpation d'identité, mise en circulation de fausses cartes...) ? Si des mesures ont été prises, quelles sont-elles ? Existe-t-il des projets visant à sécuriser son usage, lesquels ?**

Réponse : Pour autant que l'on sache, jusqu'à présent, il n'y a aucune référence à la falsification du document d'identification civile, la carte de citoyen.

6. **Existe-t-il des difficultés en matière d'accès aux soins liées spécifiquement à la mise en œuvre de mesures de sécurisation de la carte d'identité ? Des cas de non-recours voire d'exclusion de certains publics sont-ils documentés (en particulier, s'agissant de la mise en œuvre des données biométriques) ?**

Réponse : Les cas d'exclusion ou de non-respect du principe d'universalité du document sont traités et pris en compte dans la création d'alternatives et de révisions du document, lorsque cela est possible.

7. **Quelle est la procédure d'authentification suivie pour s'assurer de l'identité du patient lors de la production de la carte (chez le médecin, à l'hôpital...) :**

Réponse : Identification visuelle du document et des données qu'il contient et identification électronique en fournissant un code PIN ou une adresse d'authentification, les deux permettant l'accès aux données du document permettant d'authentifier le citoyen.

Annexe VIII

8. **Les professionnels de santé ont-ils l'obligation juridique de s'assurer de l'identité de leur patient lors de la délivrance des soins / des médicaments ? ou s'agit-il d'une obligation déontologique ? Ou n'ont-ils pas d'obligation légale/réglementaire en la matière ?**

Réponse : En vertu de de la décision du ministre de la Santé n° 1400-A/2015 du 10 février, objectif stratégique n° 5, il existe une obligation légale d'identifier les patients. En outre, la directive n°18/11 du 23 mai de la Direction générale de la santé stipule que dans les hôpitaux du Service national de santé et les services de soins de santé, l'identité des patients doit toujours être confirmée. Mais les soins de santé dans les hôpitaux et les centres publics, en particulier les cas urgents, ne sont en général pas refusés pour faute de présentation d'une carte d'identité.

9. **Les professionnels de santé (hôpital, médecin, infirmier) demandent ils systématiquement la présentation de la carte nationale d'identité (physique ou électronique) à chaque visite, ou seulement lors de l'enregistrement du patient (premier passage) ?**

Réponse : A chaque rendez-vous, pour l'identification du patient.

10. **Demande-t-on à l'assuré la saisie d'un code ou d'un mot de passe pour autoriser l'accès en lecture à la carte (soit sur le lecteur de carte ou sur le smartphone-via mail ou sms) : oui/non**

Réponse : Oui

11. **Indiquer la date de déploiement de la carte nationale d'identité comprenant le numéro de sécurité sociale, le nombre de cartes physiques en circulation (et si elle existe, le nombre de cartes dématérialisées sur smartphone).**

Réponse : La délivrance du nouveau document d'identification civile avec le numéro de sécurité sociale a commencé en 2007. Le nombre de cartes physiques, Citizen Card, en circulation est 11 Million. Le nombre de cartes (Citizen Card) dématérialisées, via ID.GOV.PT, est de 650.000.

12. **Est-il possible de mettre à jour les données biométriques (ex. si le détenteur de la carte veut référencer le pouce gauche à la place du pouce droit...), ou de les désactiver sur la carte / le support ? Dans quels cas ?**

Réponse : Actuellement, l'impression numérique avec la technologie Match-on-Card est utilisée. Il n'est pas possible de mettre à jour les données biométriques après l'émission du document.

13. **Décrire le fonctionnement du lecteur de carte (physique/dématérialisée) : nécessite-t-elle un lecteur de carte à puce / magnétique (ou saisie manuelle) ? Quelle(s) sont les technologies de lecture utilisées (scanner QR code, technologie sans contact, Bluetooth, lecteur MRZ...) ?**

Réponse : Dans le document d'identification civile à composante physique et électronique, les lecteurs de cartes à puce de contact et de lecture MRZ sont actuellement utilisés. Au cours de cette année, la technologie sans contact, la lecture MRZ et la puce de contact seront également utilisées. Dans l'ID.GOV.PT, document totalement dématérialisé intégrant le concept de porte-documents numérique, il est possible de scanner le QR code.

14. **Une même carte peut-elle servir de support pour vérifier l'ouverture des droits de plusieurs individus (famille, enfants mineurs...) ? Les enfants mineurs ont-ils une carte d'identité et un numéro de sécurité sociale dès la naissance ?**

Réponse : Non. Le document est à titre individuel et incessible.

Annexe VIII

Tous les citoyens, dès leur naissance, disposent d'une Carte de Citoyen avec un numéro d'identification d'utilisateur civil, fiscal, sanitaire et de sécurité sociale.

15. **Est-elle gratuite pour l'assuré ? y compris en cas de renouvellement anticipé (perte, vol ?) ? Quelle est sa « durée de vie » moyenne ? Quel est le coût de production moyen d'une carte ?**

Réponse : Généralement, ce n'est pas gratuit. Il a une validité de 10 ans. Toutefois, pour les nouveau-nés, elle sera gratuite jusqu'à leurs 20 premiers jours, selon l'annonce officielle publiée sur le site du gouvernement portugais.

16. **La puce de la carte nationale d'identité fait elle l'objet de mises à jour (par quel service) ?**

Réponse : La puce (chip) du document est mise à jour uniquement lors du renouvellement du document. Le contenu de la puce (chip) jusqu'en 2023 ne permettait que la mise à jour des données d'adresse.

2. Les réponses du réseau des conseillers aux affaires sociales

2.1. Le Danemark

1. **Quelles sont les caractéristiques de la carte d'assurance maladie (support des droits ouverts à l'assurance maladie obligatoire, permettant à l'assuré la prise en charge et le remboursement des frais de santé) ? Décrire son/ses format(s) : support physique, support dématérialisé (application sur téléphone mobile...)?**

La carte de santé au Danemark (*Sundhedskort*) est disponible en **support physique et en support dématérialisé (application mobile téléchargeable depuis le 1^{er} juin 2021)**. Dans les deux cas, il s'agit d'une carte de couleur jaune, ayant un code barre mais, contrairement à la carte française, elle ne comporte pas de photo du titulaire ni de puce.

On peut y lire les informations suivantes :

- Nom, prénom et adresse du titulaire
- Numéro cpr du titulaire, qui est un numéro personnel d'identification que possèdent tous les résidents au Danemark. Composé de 10 chiffres, il est utilisé comme identifiant par les administrations publiques mais également dans le secteur privé, par exemple par les banques ;
- Nom, adresse et numéro de téléphone du centre de santé/médecin référent chez qui le titulaire est inscrit ;
- Numéro de téléphone des urgences hospitalières.

La carte de santé enregistre toutes les données médicales du patient et lui permet d'accéder à tous les services publics de santé. Lors d'une consultation chez un médecin généraliste par exemple, le patient ne paie rien. Il lui suffit de passer sa carte de santé au secrétariat et il sera ainsi enregistré directement avant de se rendre à la salle d'attente.

En ce qui concerne les prescriptions médicales, l'ordonnance papier n'est plus du tout utilisée au Danemark depuis plusieurs années déjà, au profit d'un système totalement informatisé. Le patient a juste à donner au médecin sa carte de santé afin que celui-ci incorpore ses prescriptions dans un fichier informatisé, accessible également par les pharmaciens.

2. **Est-elle fusionnée avec une carte nationale d'identité ou une autre carte (préciser laquelle) ?**

Annexe VIII

Le Danemark ne dispose pas de carte nationale d'identité à proprement parler. Néanmoins, la carte de santé (ou la carte jaune comme elle est surnommée) n'est pas utilisée seulement dans le système de santé mais plus largement dans la vie quotidienne des Danois (pour justifier son identité ou son âge par exemple, emprunter des livres à la bibliothèque, etc.). De fait, elle fait donc office, en quelque sorte, de pièce d'identité.

3. Des données biométriques figurent-elles sur la carte (physique ou dématérialisée) ou une technologie biométrique est-elle utilisée pour authentifier le patient ?

Non, la carte ne comporte pas de données biométriques ni de technologies spécifiques pour authentifier le patient. Concernant l'accès à la carte dématérialisée, il faut utiliser les méthodes offertes par le smartphone pour s'identifier (code à taper ou reconnaissance faciale par exemple).

4. Si oui, la technologie biométrique est-elle utilisée à l'enrôlement (c'est-à-dire lors de la première demande de carte par le bénéficiaire, lors de la création de la carte), ou à l'usage, c'est-à-dire à chaque visite chez le professionnel de santé / à chaque passage en établissement de santé ?

Si oui, les données biométriques sont-elles présentes sur la carte et/ou sont-elles également stockées dans un fichier national ou régional centralisé ?

5. Si non, à savoir si les données de la carte d'assurance maladie ne comprennent pas de données biométriques : existe-t-il des projets / expérimentations en cours ?

Voir question suivante.

6. Existe-t-il des fraudes spécifiquement liées à l'utilisation de cette carte (usurpation d'identité, mise en circulation de fausses cartes...) ? Si des mesures ont été prises, quelles sont-elles ? Existe-t-il des projets visant à sécuriser son usage, lesquels ?

De manière générale, les sociétés nordiques, dont la société danoise, se caractérisent par un **très haut niveau de confiance entre les habitants**, avec globalement moins de délits et de fraudes à relever que dans les autres pays. Les fraudes liées à l'utilisation de la carte de santé ne semblent donc pas répandues.

Toutefois, le phénomène existe. Des débats sur ce sujet avaient surtout eu lieu quelque temps avant l'apparition de la pandémie de Covid-19. Ainsi, début 2019, la ministre de la Santé de l'époque, Ellen Trane Nørbys, avait affirmé que bien qu'il **n'existait pas de chiffres sur l'ampleur des fraudes, celles-ci devaient néanmoins être assez répandues**. Afin d'illustrer la **nécessité de moderniser la carte de santé**, Ellen Trane Nørbys avait déclaré : « Si vous perdez votre carte de santé dans la rue, vous donnez votre nom, votre adresse et votre numéro CPR à ceux qui trouvent la carte. Si les clés finissent elles aussi sur le trottoir, c'est comme si vous invitiez un inconnu à venir chez vous ». La ministre avait relevé également **les lourdeurs et le coût élevé** de la carte de santé physique, notamment parce qu'une carte est délivrée à tous les nouveau-nés et qu'elle est remplacée en cas de vol ou lorsqu'un citoyen déménage ou change de médecin.

C'est donc dans ce contexte que le projet d'une **carte de santé numérique** est apparu. Ce projet et les débats autour des possibilités de modernisation de la carte de santé ont été impulsés par un **rapport de 2019, élaboré par le cabinet de conseil en IT Lakeside et commandé par le ministère de la Santé et les régions danoises**. Il s'intitule « une carte de santé plus sûre » (*Et mere sikkert sundhedskort*).

Voici les principales conclusions et recommandations de ce rapport :

Annexe VIII

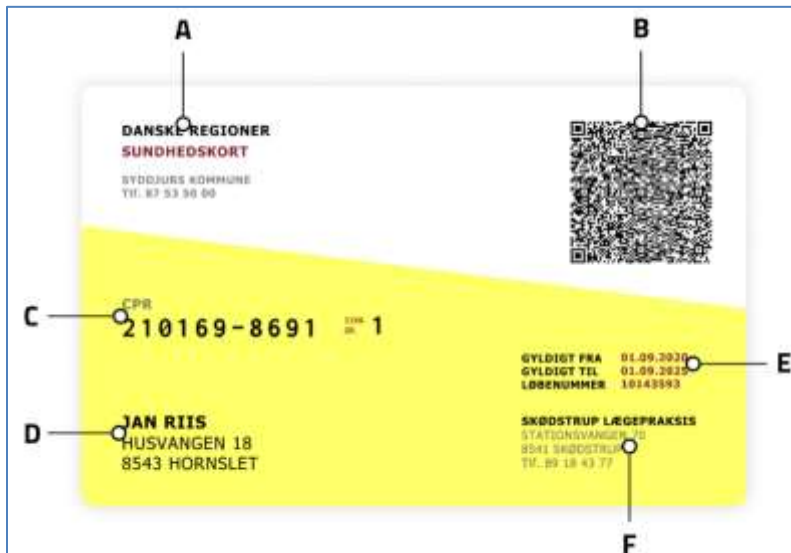
La carte de santé ne fournit **aucun moyen de s'assurer que l'individu qui la présente est le véritable titulaire**. Celle-ci est **très facile à contrefaire** à l'aide de machines à imprimer les cartes, que l'on peut se procurer à un prix relativement bas sur Internet, et il existe un **marché noir** à travers lequel une carte de santé peut être achetée pour moins de 200 DKK (environ 27€). **Il n'existe pas non plus de processus de vérification réelle de l'identité des patients**, ce qui constitue un risque puisque des personnes non autorisées pourraient avoir accès aux soins de santé gratuits.

Le rapport recommande aux autorités danoises **les deux mesures suivantes à court terme** :

La mise en place d'une nouvelle carte de santé physique

- Elle doit être sécurisée par un **code QR, un numéro de série** et une **option de blocage** (cf. proposition 1 ci-dessous).
- Coûts de mise en place : environ 35 millions de DKK (environ 4,7 millions d'euros).
- Coûts annuels supplémentaires : environ 1 million de DKK (environ 130 000 euros).

Proposition 1 de la nouvelle carte de santé physique



Source : Rapport de 2019 « Une carte de santé plus sûre » (Et mere sikkert sundhedskort).

- Une carte de santé utilisant exactement les mêmes matériaux et techniques d'impression que celle d'aujourd'hui.
- Code QR imprimé contenant toutes les données de la carte et sécurisé par une signature numérique de l'autorité émettrice. Cela rend pratiquement impossible la contrefaçon et permet aux lecteurs du code QR de vérifier la validité de la carte.
- Le numéro de CPR et le groupe de sécurité apparaissent toujours comme sur la carte actuelle.
- Il en va de même pour le nom et l'adresse du propriétaire de la carte.

Annexe VIII

- Comme nouveauté, la carte a une période de validité et un numéro de série. Une liste de blocage est créée et les cartes anciennes ou perdues sont automatiquement bloquées pour le renouvellement, l'expiration et la déclaration de perte. En outre, la possibilité d'attacher un "badge" (« mærke » en danois) à sa carte de santé est introduite ; le citoyen doit alors s'identifier avec son numéro CPR pour associer ce "badge". Les informations du badge peuvent être obtenues/contrôlées via des solutions approuvées et créent une possibilité de contrôle supplémentaire également pour les consultations téléphoniques. Le "badge" n'est pas conservé de manière centralisée, mais un "hash" du badge est stocké. En pratique, cela signifie que le badge peut être vérifié, mais ne peut être copié.
- Les nom, adresse et numéro de téléphone du centre de santé/médecin référent chez qui le titulaire est inscrit apparaissent toujours comme sur la carte actuelle.

Les auteurs du rapport proposent alternativement un **2^e type de carte**, avec une sécurité encore plus importante puisqu'elle intégrerait en plus une **photographie du propriétaire de la carte**, ainsi qu'une **puce NFC contenant des informations biométriques (la photographie)** et la possibilité de lire en toute sécurité la photographie et d'autres informations comme sur le passeport international (cf. proposition 2 ci-dessous). Les coûts de cette carte seraient nettement plus élevés que pour la proposition 1 :

Coûts de mise en place : environ 621 millions de DKK (environ 83 millions d'euros).

Coûts annuels supplémentaires : environ 116 millions de DKK (environ 16 millions d'euros).

Proposition 2 de la nouvelle carte de santé physique



Source : Rapport de 2019 « Une carte de santé plus sûre » (Et mere sikkert sundhedskort)

La mise en place d'une carte de santé numérique (cet outil a été mis en place et existe depuis juin 2021)

Le secteur de la santé doit s'associer aux initiatives en cours visant à numériser les documents officiels (voir par exemple le permis de conduire numérique sous les auspices de l'Agence danoise pour la numérisation), en vue de mettre au point une "carte de santé numérique" similaire pouvant être présentée sur un téléphone portable.

- Coûts de déploiement : environ 4 millions de DKK (environ 540 000 €).
- Fonctionnement et entretien annuels : environ 1 million de DKK (environ 130 000 €).

Annexe VIII

Comme la carte de santé actuelle est régie par un contrat de fournisseur, il pourrait être difficile de la modifier à court terme. **La solution numérique, en revanche, peut être développée et mise en œuvre immédiatement.**

Les auteurs du rapport estiment que **plus de 80 % des utilisateurs de la carte de santé seront en mesure d'utiliser la solution numérique** et que la majorité d'entre eux passeront à cette solution dans quelques années. La "**carte de santé numérique**" présente des avantages considérables : **une meilleure sécurité, une meilleure expérience utilisateur et des informations actualisées.**

Les cartes de santé physiques et numériques proposées **ne nécessiteront pas de visite auprès des autorités pour être délivrées**, et pourraient donc remplacer la carte de santé actuelle sur une **base permanente**. Selon les chiffres de l'organisation représentant les régions danoises (*Danske Regioner*), **environ 1,8 million de cartes de santé physiques sont délivrées chaque année à la suite de nouvelles arrivées, de déménagements, de changements de médecin, de pertes, etc.**

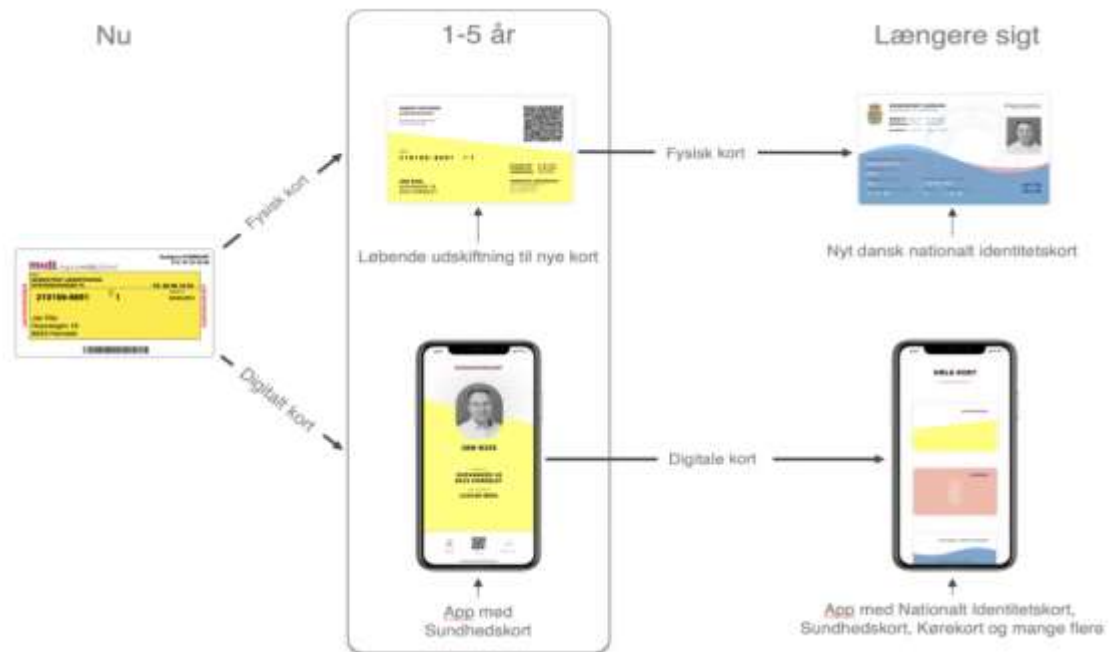
Si la **solution numérique est un grand succès** et connaît donc un taux d'adoption et d'utilisation très élevé, il convient de se demander, après la période de mise en œuvre, si **les deux solutions – physiques et numériques – ne pourraient pas être alternatives plutôt que complémentaires.**

Avec les solutions ci-dessus, le risque de fraudes dans les services de santé danois sera dans une certaine mesure, évité. Une solution encore plus performante nécessite **l'utilisation de cartes d'identité et de processus d'identification appropriés par les acteurs des soins de santé.**

Si les autorités veulent des garanties encore plus poussées contre les fraudes, les auteurs du rapport recommandent sur **le plus long terme** :

- La suppression complète de la carte de santé physique et numérique standard et son remplacement par **une nouvelle carte d'identité nationale sécurisée (physique et numérique)** avec **l'obligation d'une photo ou de mesures similaires** pour vérifier que l'individu qui présente la carte est bien son détenteur réel. Cette carte (physique ou numérique) doit être présentée lors des rendez-vous avec les prestataires de soins de santé.
- L'introduction d'une carte d'identité nationale doit être complétée par **l'amélioration des processus de vérification technique et manuelle de l'identité** par les professionnels de santé.
- Lors de l'élaboration d'une carte d'identité nationale physique, la norme 9303 de l'OACI (Organisation de l'Aviation Civile Internationale) sur les passeports devrait être consultée afin de savoir si **la carte d'identité peut également devenir un passeport électronique** pouvant être utilisé pour voyager entre les pays.
- Il conviendra de déterminer l'autorité qui sera responsable de cette carte

Résumé : évolution de la carte de santé danoise proposée par les auteurs du rapport



Source : Rapport de 2019 « Une carte de santé plus sûre » (Et mere sikkert sundhedskort).

La carte de santé actuelle apparaît à gauche du schéma. Au milieu apparaissent les propositions, pour le court terme (1-5 ans), de carte de santé physique (haut) et numérique (bas). A droite figurent, pour le plus long terme, les propositions de carte d'identité nationale physique (haut) et d'application regroupant plusieurs cartes comme la carte d'identité nationale, la carte de santé, le permis de conduire, etc. (bas).

Si, dans le domaine de la santé, le Danemark souhaite établir une **carte de santé physique et numérique avec le même nombre d'informations qu'aujourd'hui et avec une sécurité similaire à celle du permis de conduire**, les auteurs du rapport estiment que :

- Le coût de la mise en œuvre serait d'environ 621 millions de DKK (environ 83 millions d'euros).
- Le coût d'exploitation annuel serait d'environ 116 millions de DKK par an (environ 16 millions d'euros).

7. **Quelle est la procédure d'authentification suivie pour s'assurer de l'identité du patient lors de la production de la carte d'assurance maladie (chez le médecin, à l'hôpital...)**

8. **Les professionnels de santé ont-ils l'obligation juridique (légale/réglementaire) de s'assurer de l'identité de leur patient lors de la délivrance des soins / des médicaments ? s'agit-il d'une obligation déontologique ?**

Il n'existe, à notre connaissance, aucune obligation juridique ou déontologique de ce type.

9. **Comment s'assurent-ils de l'identité de leur patient ? présentation/lecture d'une carte nationale d'identité (physique ou électronique) : oui/non ; préciser si usage systématique à chaque visite, ou seulement lors de l'enregistrement du patient (premier passage), en établissement et en ville.**

L'identité du patient n'est généralement pas contrôlée.

10. S'il existe une carte d'assurance maladie : demande-t-on à l'assuré la saisie d'un code ou mot de passe préalablement à la lecture de la carte (soit sur le lecteur de carte ou sur le smartphone-via mail ou sms) : oui/non

Non.

11. Est-ce qu'il est possible pour le professionnel de santé de faire un contrôle visuel de l'identité en comparant le patient avec la photo figurant sur la carte avec son porteur : oui/non

Non.

2.2. L'Espagne

1. Quelles sont les caractéristiques de la carte d'assurance maladie (support des droits ouverts à l'assurance maladie obligatoire, permettant à l'assuré la prise en charge et le remboursement des frais de santé) ? Décrire son/ses format(s) : support physique, support dématérialisé (application sur téléphone mobile...)?

Il s'agit d'une carte de format ID3 « carte de crédit ». Elle comporte un numéro d'identification unique, propre à chaque citoyen et au système national de soins. Ce numéro est délivré, au niveau national, par le ministère de la santé.



2. Est-elle fusionnée avec une carte nationale d'identité ou une autre carte (préciser laquelle) ?

non

3. Des données biométriques figurent-elles sur la carte (physique ou dématérialisée) ou une technologie biométrique est-elle utilisée pour authentifier le patient ?

non

4. Si non, à savoir si les données de la carte d'assurance maladie ne comprennent pas de données biométriques : existe-t-il des projets / expérimentations en cours ?



non

5. Existe-t-il des fraudes spécifiquement liées à l'utilisation de cette carte (usurpation d'identité, mise en circulation de fausses cartes...)? Si des mesures ont été prises, quelles sont-elles? Existe-t-il des projets visant à sécuriser son usage, lesquels ?

Pas de fraudes récentes détectées. Le fonctionnement du système public de soins, où la personne est prise en charge gratuitement et est

rattachée à un centre de santé et à un médecin généraliste référent (sans possibilité de s'adresser à un autre médecin) limite les risques de fraude, et ce d'autant que la carte donne accès au dossier médical du patient.

En 2013, une fraude a été détectée (pour un montant d'environ 5 000€) par l'Inspection départementale des services de santé d'Almeria (Andalousie), dans un EHPAD qui utilisait les cartes sanitaires de plusieurs résidents décédés pour se procurer, en pharmacie, des médicaments qui étaient ensuite administrés à d'autres résidents.

Annexe VIII

6. **Quelle est la procédure d'authentification suivie pour s'assurer de l'identité du patient lors de la production de la carte d'assurance maladie (chez le médecin, à l'hôpital...).**

7. **Les professionnels de santé ont-ils l'obligation juridique (légale/réglementaire) de s'assurer de l'identité de leur patient lors de la délivrance des soins / des médicaments ? s'agit-il d'une obligation déontologique ?**

Non.

8. **Comment s'assurent-ils de l'identité de leur patient ? présentation/lecture d'une carte nationale d'identité (physique ou électronique) : oui/non ; préciser si usage systématique à chaque visite, ou seulement lors de l'enregistrement du patient (premier passage), en établissement et en ville**

Non, présentation de la carte sanitaire.

9. **S'il existe une carte d'assurance maladie : demande-t-on à l'assuré la saisie d'un code ou mot de passe préalablement à la lecture de la carte (soit sur le lecteur de carte ou sur le smartphone-via mail ou sms) : oui/non.**

Il n'existe pas de carte d'assurance-maladie.

10. **Est-ce qu'il est possible pour le professionnel de santé de faire un contrôle visuel de l'identité en comparant le patient avec la photo figurant sur la carte avec son porteur :**

Non.

11. **Autre(s) mesure(s) d' « identitovigilance » (mesure visant à authentifier l'identité du patient dans un objectif de sécurité sanitaire des soins) éventuellement mise(s) en œuvre lors d'une visite chez un professionnel de santé/accueil par un établissement ? si oui préciser**

Néant.

2.3. La Suède

1. **Quelles sont les caractéristiques de la carte d'assurance maladie (support des droits ouverts à l'assurance maladie obligatoire, permettant à l'assuré la prise en charge et le remboursement des frais de santé) ?**

Il n'existe pas en Suède de carte d'assurance maladie. Il n'existe pas en Suède de système d'assurance maladie semblable au système français ni de système de « mutuelles ».

2. **Quelle est la procédure d'authentification suivie pour s'assurer de l'identité du patient lors de la production de la carte d'assurance maladie (chez le médecin, à l'hôpital...).**

/

3. **Les professionnels de santé ont-ils l'obligation juridique (légale/réglementaire) de s'assurer de l'identité de leur patient lors de la délivrance des soins / des médicaments ? s'agit-il d'une obligation déontologique ?**

Les professionnels de santé ont l'obligation réglementaire de s'assurer à chaque fois de l'identité du patient. Le contrôle doit avoir lieu sur présentation d'une pièce d'identité approuvée.

Pendant les soins continus en hospitalisation, il suffit que le personnel soignant confirme verbalement l'identité du patient et en vérifiant le bracelet d'identification.

Annexe VIII

4. **Comment s'assurent-ils de l'identité de leur patient ? présentation/lecture d'une carte nationale d'identité (physique ou électronique) : oui/non ; préciser si usage systématique à chaque visite, ou seulement lors de l'enregistrement du patient (premier passage), en établissement et en ville.**

En Suède, la quasi-majorité des personnes adultes présentent leur permis de conduire comme pièce d'identité, systématiquement à chaque visite. L'élément principal pour authentifier le patient est le « **personnummer** » ou numéro personnel « année – mois – jour – XXXX », composé de la date de naissance et de 4 chiffres individuels. Ceux qui n'ont pas de permis de conduire utilisent la carte d'identité qui contient également le personnummer.

Les personnes étrangères peuvent prouver leur identité en présentant leur carte d'identité ou leur passeport.

À titre d'exemple, dans les régions de Stockholm et de Gotland, les systèmes de « journaux patients » sont connectés au registre régional des données personnelles («*personuppgiftsregistret*») qui lui-même tire des données du registre national de la population («*folkbokföringsregister*»)

Le registre national de la population est géré par l'agence des impôts (*Skatteverket*) et contient des informations telles que : numéro personnel, nom, dates de naissance et de décès, sexe, adresse, statut, citoyenneté, nom des parents / enfants / époux, entre autres.

Une personne qui ne peut pas ou ne veut pas prouver son identité peut donc devoir payer elle-même la totalité des frais.

5. **S'il existe une carte d'assurance maladie : demande-t-on à l'assuré la saisie d'un code ou mot de passe préalablement à la lecture de la carte (soit sur le lecteur de carte ou sur le smartphone-via mail ou sms) : oui/non**

/

6. **Est-ce qu'il est possible pour le professionnel de santé de faire un contrôle visuel de l'identité en comparant le patient avec la photo figurant sur la carte avec son porteur : oui/non**

/

7. **Autre(s) mesure(s) d'« identitovigilance» (mesure visant à authentifier l'identité du patient dans un objectif de sécurité sanitaire des soins) éventuellement mise(s) en œuvre lors d'une visite chez un professionnel de santé/accueil par un établissement ? si oui préciser**

Le numéro personnel « personnummer »

2.4. Les Etats-Unis d'Amérique

1. **Quelles sont les caractéristiques de la carte d'assurance maladie (support des droits ouverts à l'assurance maladie obligatoire, permettant à l'assuré la prise en charge et le remboursement des frais de santé) ?**

- Décrire son/ses format(s) : support physique, support dématérialisé (application sur téléphone mobile...)?

Annexe VIII



- La carte d'assurance maladie dépend du régime auquel on est rattaché. Les multiples assurances privées peuvent utiliser des supports très divers, plus ou moins sophistiqués. Ce qui se rapprocherait le plus de notre carte vitale sont les cartes délivrées par Medicare

(plus de 65 ans et handicapés) avec plus de 62 millions d'adhérents ou celui du département des Veterans (VA, 9 millions d'adhérents).

- La carte Medicare est aujourd'hui une carte sous format papier. Jusqu'en 2018, elle intégrait le numéro de sécurité sociale (*Social Security Number* (SSN) à 9 chiffres). Le SSN est un numéro d'immatriculation unique et confidentiel. Pour des raisons de fraude, ce numéro n'apparaît plus suite à une recommandation de 2012 ([GAO 12-831](#)). Le Medicare Beneficiary Identifier (MBI), a remplacé les numéros de sécurité sociale à 9 chiffres qui identifiaient les personnes inscrites. Pour la VA, une carte à piste magnétique est utilisée.
- La question du passage à une carte électronique avec le cas échéant des éléments d'authentification complémentaire (photo ou biométrie) a fait l'objet d'une étude approfondie en 2015 du Government Accountability Office « *Medicare- Potential Uses of Electronically Readable Cards for Beneficiaries and Providers* » ([gao-15-319.pdf](#)). Ce rapport s'est notamment fondé sur des échanges avec les administrations française et allemande pour évaluer les bénéfices et les coûts induits par la mise en place d'une carte « électronique ».



- Ses conclusions se sont avérées négatives sur le passage à un support électronique du fait notamment des

réticences de l'administration des CMS (rattachée au HHS, en charge des liens avec les établissements de santé et médico-sociaux, de la supervision de Medicare ...). Ces réticences reposaient notamment sur le coût organisationnel de mise en place, sur les coûts de fonctionnement d'un système de carte type carte vitale, sur les craintes que ce dispositif entrave l'accès aux soins de publics fragiles, sur les risques de fraude résiduelle élevée, sur l'analyse des limites des expériences française et allemande. Les CMS ont alors clairement indiqué aux rapporteurs du GAO qu'ils ne conditionneraient pas la prise en compte des demandes de remboursement à l'utilisation d'une carte électronique si elle était mise en place pour ne pas risquer de limiter l'accès aux soins.

Annexe VIII

- Différentes législatures d'Etat ont depuis étudié la possibilité de réaliser cette transformation pour la gestion de leurs prestations Medicaid (*assurance santé pour les plus démunis*) mais ont renoncé principalement sur la base du rapport du GAO de 2015 et d'autres considérations locales. Ainsi l'Etat de Louisiane en 2020 a décliné cette perspective dans le cadre d'une demande d'information des législateurs sur un système de lutte contre la fraude à Medicaid [LaVerify System](#).
- La pandémie a cependant créé un nouveau contexte, plusieurs Etats ayant mis en place des « *Smart Health Cards* » de vaccination du fait de la faible fiabilité des « cartes de vaccination » en format papier. Les systèmes des Etats de New York ou de Californie ont ainsi été adoptés dans plusieurs Etats. Les cartes des parents ont intégré dans un second temps les informations relatives à leurs enfants. Les *Smart Health Card* sont une technologie qui permet aux Américains de conserver une copie de leurs informations sur le vaccin et le test COVID sous forme de code. Désormais utilisées dans plus de 20 États, elle rend les informations sanitaires plus faciles à vérifier et plus difficiles à falsifier. Grâce à ce système, les entreprises et les institutions peuvent facilement vérifier l'authenticité d'un dossier de santé, comme le statut vaccinal d'un individu.
- Dans le cadre des efforts en cours pour améliorer l'interopérabilité des systèmes d'information en santé sur le territoire américain, les CMS-ONC-HHS devraient probablement se pencher prochainement sur de possibles évolutions.
- La carte de sécurité sociale pour sa part n'a pas pour vocation de rembourser les frais médicaux. Elle peut être commandée via une procédure en ligne sur le site de la *Social Security Administration*. Elle est au format papier, ce qui ne manque pas de poser également des problèmes de sécurité.
- Est-elle fusionnée avec une carte nationale d'identité ou une autre carte (préciser laquelle) ?
 - Les numéros qui composent le SSN permettent donc un accès à diverses procédures administratives aux Etats-Unis. Mais il n'y a pas de fusion à proprement parler.
- Des données biométriques figurent-elles sur la carte (physique ou dématérialisée) ou une technologie biométrique est-elle utilisée pour authentifier le patient ?
 - **L'absence de carte vitale** sur le territoire américain n'empêche pas l'ouverture d'une discussion autour de données biométriques dématérialisées par les autorités de santé américaines ces dernières années. La biométrie est un secteur qui séduit un nombre croissant de professionnels de santé américains ces dernières années et fait l'objet de nombreuses expérimentations (*scanners d'empreintes digitales, les lecteurs de veines de la paume, les technologies de reconnaissance faciale ou scanners d'iris*).
 - La **biométrie** (*empreinte digitale surtout*) est déjà utilisée dans le milieu hospitalier. Elle permet aux médecins de se connecter à leur poste de travail, d'alléger les temps d'attente des patients, de contribuer à la qualité de l'expérience patient. Un scénario qui utilise la vérification en temps réel de l'ADN à l'aide de la salive est évoqué pour les prochaines années.

Annexe VIII

- Un élément important pour la biométrie est la nécessité d'un **cadre législatif**. Alors que les établissements de santé s'efforcent de fournir aux patients une expérience d'enregistrement et d'authentification sans friction, il est essentiel de s'assurer que la technologie soit conforme aux injonctions de confidentialité des données et de vie privée. Au niveau législatif, les données biométriques entrent dans la catégorie des informations de santé protégées (PHI). Les établissements médicaux doivent protéger ces données conformément à la loi HIPAA (Health Insurance Portability and Accountability Act), à la loi HITECH (Health Information Technology for Economic and Clinical Health) et à d'autres réglementations applicables dans leur pays d'activité. Actuellement, cinq États américains ont adopté le projet de *Biometric Information Privacy Act* (BIPA) de 2008. D'autres États sont toujours en train d'en débattre.

Projets, expérimentations en cours :

Nous n'avons pas connaissance d'expérimentations en cours pour les cartes d'assurance maladie des assurances publiques. La plupart des mises en œuvre concernent les systèmes de santé locaux.

- Chez **Northwell Health**, le plus grand prestataire de soins de santé de l'État de New York, le déploiement des scans biométriques en 2018 visait à intégrer la technologie de reconnaissance de l'iris et du visage dans diverses fonctions du système hospitalier. Le système, qui a vu la participation d'environ 50 000 patients, pourrait ajouter la reconnaissance vocale comme couche supplémentaire d'identification.
 - Le concept a également pris son essor au centre médical de **l'Université de Pittsburgh (UPMC)**, qui a d'abord mis en place des scanners d'empreinte digitale en 2016 afin de réduire le temps d'enregistrement des patients. Aujourd'hui, l'UPMC entretient 3 800 lecteurs biométriques répartis sur 68 sites. À ce jour, plus de 630 000 empreintes digitales ont été enregistrées.
 - Existe-t-il des fraudes spécifiquement liées à l'utilisation de cette carte (usurpation d'identité, mise en circulation de fausses cartes...) ? Si des mesures ont été prises, quelles sont-elles ? Existe-t-il des projets visant à sécuriser son usage, lesquels ?
 - La **carte Medicare** fait régulièrement l'objet de cas de fraude favorisés par la fragilité du public concerné. Une escroquerie fréquente consiste à proposer une carte à puce en plastique aux bénéficiaires de Medicare pour remplacer la carte d'identité papier en donnant son numéro d'identification Medicare.
 - Pour remédier aux fraudes, un numéro spécial ainsi qu'une plateforme dédiée ont été mis en place sous l'impulsion des CMS pour signaler les escroqueries et sensibiliser les populations, surtout âgées.
 - *L'Affordable Care Act de 2010* couvre également la prévention des fraudes à l'assurance maladie. À l'issue de son adoption, les CMS ont mis en place un *Fraud Prevention Toolkit* pour prévenir les fraudes (source : HHS <https://www.hhs.gov/guidance/document/fraud-prevention-toolkit-0>),
 - Les CMS ont aussi mis en place la campagne *Guard Your Card*, demandant de signaler toute activité suspecte, par exemple lorsqu'on leur demande par téléphone leur numéro de Medicare/Sécurité sociale ou des informations bancaires.
2. **Quelle est la procédure d'authentification suivie pour s'assurer de l'identité du patient lors de la production de la carte d'assurance maladie (chez le médecin, à l'hôpital...)**
- Les professionnels de santé ont-ils l'obligation juridique (légale/réglementaire) de s'assurer de l'identité de leur patient lors de la délivrance des soins / des médicaments ? s'agit-il d'une obligation déontologique ?

Annexe VIII

- Nous n'avons pas identifié de base légale, réglementaire ou déontologique d'une telle obligation juridique tant au niveau fédéral que des Etats. Les professionnels de santé ont une forte incitation néanmoins à s'assurer de la conformité à l'identité validée lors de l'admission pour des raisons de sécurité des soins. Mais le contrôle lors de la consultation se fait habituellement par simple interrogatoire sauf pour les établissements ayant déjà mis en place des technologies innovantes ou pour les patients hospitalisés par la vérification du bracelet d'identification. En ce qui concerne l'identification initiale, elle est du ressort des personnes chargées des admissions. Elle peut se limiter à la vérification de la carte d'adhérent à une assurance santé et celle d'une pièce d'identité si le patient en dispose d'une.
- En l'absence de carte vitale, la vérification de l'identité du patient intervient avant qu'un patient puisse accéder aux soins de santé, par exemple en prenant un rendez-vous par téléphone ou en commandant une nouvelle ordonnance. Les établissements de santé doivent s'assurer que les dossiers médicaux et les informations d'assurance correspondent au bon patient.
- Une loi fédérale récente (2021) visant à lutter contre l'abus de prescription d'opioïdes exige que les médecins envoient aux pharmacies des ordonnances numériques, et non en papier, pour les substances contrôlées et qu'ils se conforment aux règles et normes de la Drug Enforcement Administration (DEA). La DEA exige une authentification à deux facteurs pour authentifier l'identité du prescripteur. Les prescripteurs saisissent un code aléatoire généré par un badge disponible, puis un lecteur authentifie l'identité de la personne et son autorisation de prescrire.
- Comment s'assurent-ils de l'identité de leur patient ? présentation/lecture d'une carte nationale d'identité (physique ou électronique) : oui/non ; préciser si usage systématique à chaque visite, ou seulement lors de l'enregistrement du patient (premier passage), en établissement et en ville
 - L'identité est généralement vérifiée par la présentation du permis de conduire ou du passeport. Il n'existe pas de carte nationale d'identité avec photographie. Certains Etats ont mis en place des state cards, notamment pour les personnes qui ne conduisent pas. Mais de nombreux cas de fraude ont abouti à une législation en 2005 (the Real ID Act) renforçant les exigences concernant l'émission de ces papiers d'identité par les Etats. Mais, la mise en œuvre n'était pas encore systématique fin 2022. Sous la pression des transporteurs aériens, ces cartes sécurisées seront obligatoires à compter du 3 mai 2023 pour tout vol domestique.
 - Les pratiques ne sont pas standardisées sur la vérification à chaque visite. Elle se limite cependant le plus souvent au premier passage dans la plupart des centres de santé. Elle est plus courante dans les bureaux des admissions des hôpitaux pour des raisons de facturation. Elle n'est en aucun cas systématique sur le territoire américain.
- S'il existe une carte d'assurance maladie : demande-t-on à l'assuré la saisie d'un code ou mot de passe préalablement à la lecture de la carte (soit sur le lecteur de carte ou sur le smartphone-via mail ou sms) : oui/non
 - La carte d'assurance maladie est au format papier pour Medicare et le plus souvent pour Medicaid. Il n'y a pas de code ou de mot de passe requis. Pour la carte à bande magnétique des Veterans, pas de mot de passe requis.
- Est-ce qu'il est possible pour le professionnel de santé de faire un contrôle visuel de l'identité en comparant le patient avec la photo figurant sur la carte avec son porteur : oui/non

Annexe VIII

- Non pour Medicare. Le contrôle d'identité se fait davantage par l'interrogation d'une base de données rattachée au Patient ID. Oui pour la carte Veteran (VHIC).
- Autre(s) mesure(s) d' « identitovigilance » (mesure visant à authentifier l'identité du patient dans un objectif de sécurité sanitaire des soins) éventuellement mise(s) en œuvre lors d'une visite chez un professionnel de santé/accueil par un établissement ? si oui préciser

Dans le cadre des soins pour un patient déjà admis, la méthode la plus courante consiste à demander aux patients de réciter leur nom et leur date de naissance pendant que les infirmières et les médecins les comparent à un bracelet ou à un numéro de dossier porté au poignet. De plus, des erreurs d'écriture au cours du processus d'enregistrement peuvent entraîner des erreurs médicales potentielles. Ce problème très répandu a conduit la Joint Commission (organisme d'accréditation équivalent sur le champ de notre HAS) à déclarer cette question comme l'un des principaux objectifs en matière de sécurité des patients.

ANNEXE IX

Contributions écrites

Pièce jointe 1

Contribution de la FHF

Mission IGAS portant sur la mise en place d'une carte vitale biométrique Retour FHF

Le 17/02/2023

Objet : Retour de la FHF suite à l'audition par l'IGAS le 25 janvier 2023

La FHF a été auditionnée le 25 janvier 2023 au sujet du projet de mise en place d'une carte vitale biométrique. Cette mission a pour projet d'évaluer l'opportunité et la faisabilité de ce projet, et notamment son intégration dans le processus d'admission à l'hôpital.

1. Un sujet important qui s'intègre dans une politique d'identitovigilance plus large

Le sujet de l'identité à l'hôpital est un élément primordial de la sécurité des soins à l'hôpital. Depuis plusieurs années, les établissements de santé ont mis en place un arsenal de procédures de vérification et de contrôle de l'identité afin de garantir la sécurité des patients. L'identitovigilance fait partie des domaines contrôlés inscrits dans les versions successives du manuel de certification des établissements de santé publié par la Haute Autorité de Santé (HAS) depuis la V2010.

Le sujet de l'identitovigilance est un enjeu en constante évolution compte-tenu du développement du numérique et de la convergence des systèmes d'information. Ainsi, toute démarche relative à la gestion de l'identité ou au rapprochement de deux identités peut avoir des conséquences sur le traitement des dossiers patients. L'identitovigilance connaît également une réglementation en évolution : la mise en place récente de l'identifiant national en santé a été accompagnée d'un nouveau référentiel d'identitovigilance en vigueur depuis le 27 mai 2021¹ qui clarifie et unifie les règles pour tous les établissements.

La question de l'usurpation de l'identité est un enjeu essentiel de la politique d'identitovigilance et fait l'objet d'un traitement dédié au sein de celle-ci (voir exemples de procédures relatives à l'usurpation). Pour autant, la fréquence du risque s'avère faible tout comme le nombre d'événements indésirables traités. En effet, les établissements sont plutôt concernés par les risques d'erreur ou de collision d'identité, qui conduirait à prodiguer le mauvais soin au mauvais patient ou à intégrer une donnée médicale dans le dossier d'un autre patient. Chaque établissement connaît des dizaines d'événements indésirables portant sur des erreurs d'identité, plutôt que sur des actions délibérées.

Pour autant, l'usurpation d'identité comporte un véritable risque pour le patient. En effet, si l'équipe se réfère à un dossier médical qui n'est pas celui du patient, cela peut engendrer des conséquences importantes sur les décisions médicales à prendre.

Du point de vue des établissements, le sujet de l'usurpation d'identité est donc davantage une question relative à l'identité et à ses répercussions médicales, qu'au regard de la prise en charge du patient, bien que ce sujet en soit la source. En effet, les rares cas d'usurpation avérés sont souvent la conséquence d'une absence de droit à la sécurité sociale de la personne concernée.

2. Un sujet qui n'est pas primordial au regard des priorités en termes de recouvrement

Comme indiqué, le sujet de l'usurpation est davantage pris en compte en matière de risque médical.

¹ Arrêté du 27 mai 2021 portant approbation des modifications apportées au référentiel « Identifiant national de santé »

Sur un plan financier, le principal risque auquel est confronté un établissement est celui du recouvrement. Ainsi, les établissements accueillent chaque jour des patients dénués de droits à sécurité sociale, souvent insolvable, et qui ne laissent que peu d'éléments permettant la bonne facturation. Ces situations conduisent les trésoreries à constater l'insolvabilité des débiteurs et l'impossibilité à maintenir les poursuites, et les factures ne sont pas honorées. Entre 2012 et 2019, le taux d'admissions en non-valeur des établissements publics de santé (compte 654) a augmenté de 69%, passant de 141 M€ en 2012 à 230 M€ en 2019². Il est à noter que les ANV ne sont pas exclusivement liés aux patients sans droits. Pour autant, cette évolution à la hausse doit interroger.

Ces situations d'irrecouvrabilité, portées par les établissements publics de santé qui assument la charge de ces créances, peuvent trouver différentes origines :

- **Des patients dont la situation n'entre pas dans les conditions des différents dispositifs de protection.** Le dispositif de l'Aide médicale d'Etat (AME) exige une présence minimale de trois mois sur le territoire que le patient ne peut systématiquement justifier : toute hospitalisation antérieure à la demande est donc à ses frais. Le dispositif de soins urgents est quant à lui limité aux situations d'urgences et ne capte pas l'ensemble des pathologies.
- **Un refus de la part des assurances voyages de prendre en charge les frais de santé :** c'est notamment le cas pour les patients dont la maladie était préalablement connue mais non déclarée auprès de l'assurance voyage.
- **Une méconnaissance des dispositifs sociaux qui conduit à ce que certains patients ne fassent pas de demande de droits.** Ainsi en 2018, la DREES établissait que le taux de recours à la CMU-C était estimé entre 56 % et 68 %, tandis que celui de l'ACS était alors estimé entre 33 % et 47 %³. L'IGAS, dans son rapport portant sur l'AME cite une étude indiquant que seules 51 % des personnes qui y sont éligibles bénéficiaient de l'AME en 2019⁴. Par ailleurs, ces situations, lorsqu'elles sont découvertes par le service social de l'établissement, sont parfois anciennes et ne permettent pas une rétroactivité suffisante pour couvrir l'ensemble des factures

Les établissements de santé sont ainsi le réceptacle de toutes ces situations d'exclusion des dispositifs de protection sociale.

Loin d'être une situation de préoccupation majeure pour les établissements de santé sur le plan financier, l'usurpation d'identité est plutôt la conséquence d'une situation d'exclusion de dispositifs sociaux qui oblige le patient à contourner les règles pour accéder aux soins.

3. Une proposition qui s'intègre mal dans le fonctionnement actuel des admissions

Les différents dispositifs portés dans le cadre du programme Simphonie portés par la DGOS visent à fluidifier et faciliter le parcours administratif du patient. L'objectif est ainsi d'automatiser ce qui peut l'être et de concentrer le travail des bureaux des entrées sur les tâches à plus forte valeur ajoutée. A ce programme s'ajoutent de nombreuses évolutions techniques proposées par les éditeurs de gestion administrative du malade (GAM) qui ont permis de faciliter, d'automatiser et d'accélérer les admissions, tout en renforçant les contrôles. Ils ont également permis le développement de la préadmission et de la préadmission en ligne.

Dès lors, ce projet paraît à **contre-courant par rapport à l'objectif de simplification de la chaîne administrative et aux parcours de plus en plus numérisés des patients**, et à la politique de dématérialisation menée par la CNAM et la DGOS (encouragement à l'usage de CDRI pour limiter les taux de rejets, et bientôt l'appli carte vitale pour les patients, qui ne prévoit pas de prise d'empreinte). Les établissements ont favorisé une organisation de leurs services en back office, afin de développer les préadmissions pour les parcours programmés, et voient de moins en moins le patient, ils n'auront donc guère l'usage de cette carte biométrique.

² Bases finances DGFIIP, FHF Data

³ Le non-recours aux prestations sociales, DREES, juin 2020

⁴ L'aide médicale d'Etat : diagnostic et propositions, IGAS-IGF, octobre 2019

Enfin, pour certains établissements, la fraude hospitalière ne passe plus réellement par la carte vitale, puisque les établissements utilisent davantage CDRI, mais par une usurpation d'identité émise par le patient.

La mise en œuvre de ce projet conduira donc mécaniquement à :

- Réintroduire un passage obligatoire par le bureau des entrées qui conduirait à revenir en arrière sur la politique de simplification du parcours administratif du patient et à renforcer la lourdeur ;
- A mettre en place de nouveaux outils de contrôle (empreintes digitales, reconnaissance faciale) ce qui alourdirait le processus d'admission ;
- A générer un surcoût en ressources humaines et en systèmes d'information qui ne feront a priori l'objet d'aucune compensation ;
- A augmenter le temps d'admission au détriment du temps de soins.

La FHF s'interroge sur le réel impact financier positif que permettrait un tel dispositif au regard de l'ensembles des coûts générés par cet outil (fabrication de la carte, relevé d'empreintes, coûts RH etc.), notamment les coûts indirects pour les établissements de santé.

4. Un sujet porteur de risques

En complément, la FHF tient à souligner deux risques majeurs à la mise en place de ce dispositif.

Une modification de la mission d'accueil inconditionnel de l'hôpital public

Les établissements publics de santé accueillent de façon inconditionnelle tout patient, sans tenir compte des ses modalités de prise en charge. Cette caractéristique d'accueil indéfectible emporte des conséquences financières potentielles déjà évoquées.

Le sujet du contrôle de la prise en charge sécurité sociale et complémentaire est perçu comme une étape administrative superflue et secondaire du point de vue de la mission de soins de l'établissements, bien qu'elle soit essentielle sur le plan financier.

Les établissements publics de santé sont tenus de s'assurer de l'identité d'un patient d'un point de vue médical et d'enregistrer les informations relatives à la prise en charge telles qu'elles sont transmises. Pour autant, **un établissement n'est pas en droit d'exiger une pièce d'identité d'un patient si ce dernier refuse de la présenter**, ni d'interdire l'accès aux soins.

La mise en place de ce projet conduirait à **modifier la mission des hôpitaux publics et leur confèreraient une mission de police**. En effet, au-delà de la vérification des traits de l'identité, les établissements contrôlèrent l'usurpation potentielle de droits et le déclareraient auprès de l'assurance maladie. On peut également s'interroger sur les conséquences de cette organisation : l'accès aux soins doit-il être interdit à un patient dans cette situation ? Il s'agit donc d'une modification profonde de la mission primordiale de soins.

Un risque de renoncement aux soins

En cas de mise en place d'une politique restrictive pour limiter les risques de fraude, il existe un risque plus important de renoncement aux soins par crainte de la dénonciation. Les enjeux financiers font toujours partie des motifs potentiels de renoncement aux soins⁵.

⁵ *Le non-recours aux prestations sociales*, DREES, juin 2020

Pièce jointe 2

Contribution de l'Ordre National des Médecins



ORDRE NATIONAL DES MÉDECINS
Conseil National de l'Ordre

M. Vincent RUOL
Inspecteur général
IGAS
39-43 quai André Citroën
75739 PARIS CEDEX 15
vincent.ruol@igas.gouv.fr

Docteur René-Pierre LABARRIERE
Président de la Section Exercice Professionnel

Paris, le 15 février 2023

CNOM/2022/12/08-020
(à rappeler dans toutes correspondances)
Section Exercice Professionnel
RPL/MT/CP/EP
Courriel : exercice-professionnel.cn@ordre.medecin.fr
Tél : 01 53 89 33 32 / 32 85 / 59

Objet : Carte vitale

Monsieur l'Inspecteur général,

Je fais suite à notre rencontre du 4 janvier dernier dans les locaux du CNOM concernant le projet d'une carte vitale biométrique et vous remercie à nouveau pour cet échange.

Nous vous avons rappelé à cette occasion que les médecins ont pour mission de prendre en charge les malades dans un cadre de confiance mutuelle. La lutte contre la fraude à l'assurance maladie par les assurés sociaux, dont la légitimité est incontestable, ne relève pas des missions des médecins mais des organismes d'assurance maladie et des autorités judiciaires.

Comme nous vous l'avons indiqué, la procédure dite du « flux dégradé » permet, en tout état de cause, la prise en charge médicale nonobstant l'absence de carte vitale.

Concernant la mise en place de l'Identifiant National de Santé, le Conseil national a considéré que :

- la bonne identification du patient est un facteur clé de la sécurité de son parcours de santé ainsi que de la qualité et de la sécurité des soins. Dans certains cas, une erreur d'identification peut conduire à des événements indésirables graves ;
- dans le cadre de l'identitovigilance, les médecins, ou les personnes sous leur autorité, ne contrôlent pas l'identité mais vérifient, le cas échéant, que l'INS correspond bien aux éléments d'identité du patient. Il s'agit de « qualifier l'INS ».

4, rue Léon Jost – 75855 Paris Cedex 17
Tél. 01.53.89.32.00
<https://www.conseil-national.medecin.fr>

Pièce jointe 2

En revanche, le projet de mise en place d'un dispositif de contrôle de biométrie, au sein des cabinets médicaux est incompatible avec la relation de confiance indispensable aux soins. De plus, ce dispositif est de nature à augmenter les incivilités et agressions à l'encontre des médecins de même qu'à les surcharger de tâches non médicales, alors que les pouvoirs publics eux-mêmes entendent lutter contre ce fléau.

Je vous prie d'agréer, Monsieur l'Inspecteur général, l'expression de mes salutations les meilleures.

Docteur René-Pierre LABARRIERE
Président de la Section Exercice Professionnel

4, rue Léon Jost – 75855 Paris Cedex 17
Tél. 01.53.89.32.00
<https://www.conseil-national.medecin.fr>

Les données personnelles nécessaires à l'accomplissement des missions de l'Ordre des médecins sont traitées dans des fichiers destinés à son usage exclusif. Conformément au Règlement Général sur la Protection des Données, les personnes concernées disposent d'un droit d'accès, de rectification, de portabilité, d'opposition et d'effacement des données les concernant, qu'elles peuvent exercer par courrier postal ou par courrier électronique.

Pièce jointe 3

Contribution du Conseil National de l'Ordre des Pharmaciens

Enquête de l'IGAS

Contribution du Conseil National de l'Ordre des Pharmaciens

Nous avons bien pris note des éléments que vous nous avez transmis le 7 décembre 2022 et des échanges complémentaires que nous avons eus le 17 janvier 2023.

Nous confirmons qu'en l'état le projet de carte vitale biométrique ne nous semble pas avoir démontré son intérêt spécifique, notamment compte tenu du déploiement prévu par l'Assurance Maladie de l'appli carte vitale sur smartphone, qui est intégrée au volet numérique du Ségur de la santé.

De fait, ce projet de carte vitale biométrique soulève plus de questions qu'il n'apporte de réponses. Vous trouverez ci-dessous nos principaux questionnements par rapport aux thèmes sur lesquels nous avons échangé.

Faisabilité de la mise en place d'une carte vitale biométrique / aspects liés à l'exercice professionnel, en particulier en officine

Les questionnements au niveau de l'Ordre sont les suivants :

● Prérequis 1 : fonctionnement

- ▶ Est-elle inscrite dans les évolutions prévues de la Feuille de route du numérique en santé 2023-2027 ?
- ▶ Comment va se présenter cette carte physiquement ?
- ▶ Comment la carte va-t-elle être contrôlée par le logiciel de gestion de l'officine ?

● Prérequis 2 : technique

- ▶ Quel élément de biométrie va être présent sur la carte ?
- ▶ Quels seront les prérequis techniques pour les logiciels de PS ? (nécessiteront-ils un changement de lecteurs de cartes ?)
- ▶ Y aura-t-il une garantie supplémentaire au sens sécurité par rapport à l'appli carte Vitale ?

● Impacts sur l'exercice professionnel en officines

- ▶ Comment la carte va-t-elle gérer la notion d'ayants droit ?
- ▶ Quelle articulation est envisagée par l'**assurance maladie** entre l'utilisation de cette carte et la **procédure médicaments onéreux**¹ en vigueur depuis le 24 octobre 2022 ?

Cette mesure, renforçant les missions de vérification du pharmacien dans le cadre de la dispensation de médicaments onéreux, a été prévue dans le cadre de la nouvelle convention pharmaceutique. Il est précisé dans la procédure, qu'elle *ne doit en aucun cas conduire à des discriminations entre les patients, ni de limiter leur accès aux soins.*

¹ <https://www.ameli.fr/seine-et-marne/pharmacien/exercice-professionnel/delivrance-produits-sante/regles-delivrance-prise-charge/fraude-medicaments-onereux-controle-renforce>



- ✓ Cette procédure ne vise que l'authentification de l'ordonnance : s'il s'avère que l'ordonnance est frauduleuse, le pharmacien refuse la délivrance et inscrit sur l'ordonnance « Refus de délivrance » et transmet une copie au service médical.

En revanche, si l'ordonnance est authentifiée, le pharmacien mentionne sur l'ordonnance qu'il a vérifié son authenticité en y inscrivant « Délivrance sécurisée » avant de transmettre une copie à l'Assurance Maladie.

Pour les ordonnances émises par un professionnel de santé libéral ou salarié d'un centre de santé, en l'absence d'information permettant de confirmer l'authenticité de l'ordonnance, le pharmacien délivre le conditionnement minimal associé au traitement. Il inscrit alors sur l'ordonnance « Délivrance temporaire » et poursuit ses vérifications : il peut notamment prendre contact avec le professionnel de santé libéral prescripteur, s'il n'a pas encore eu lieu, dans le laps de temps entre cette délivrance et son renouvellement éventuel.

- ✓ Cette mesure s'inscrit dans le cadre de la lutte contre les fraudes aux médicaments onéreux remboursables par l'Assurance Maladie.

- **Planning**

- ▶ Quels sont les plannings prévisionnels de développement et de déploiement ?

Faisabilité de la mise en place d'une carte vitale biométrique / aspects éthiques, dans le cas du refus de soins que pourrait engendrer un défaut d'identification

- **Finalité**

- ▶ Quelle est la finalité de la mise en place d'une telle carte biométrique ? Renforcer l'identification du patient, lutter contre la fraude...? Si oui, quel rôle est attendu des pharmaciens d'officine au niveau du dialogue avec les patients qui se présentent et des décisions à prendre ?
- ▶ Quelle est la population cible de cette nouvelle génération de carte, sachant que la CNAM déploie également l'apCV (carte vitale sur smartphone) ?

- **Cohabitation carte Vitale actuelle et appli carte Vitale**

- ▶ La carte Vitale biométrique est-elle destinée à remplacer la carte Vitale actuelle ?
- ▶ Quel recouvrement fonctionnel avec l'appli carte Vitale ?

- **D'un point de vue de l'éthique et des choix laissés à l'assuré, il nous semble que deux scénarios peuvent s'envisager :**

- ▶ Coexistence carte Vitale physique (ancienne ou biométrique) et appli carte Vitale >> le plus cher pour l'Assurance maladie
- ▶ Choix par le patient entre carte Vitale physique et appli carte Vitale >> le plus économique

- D'un point de vue sécurité, les deux scénarios ci-dessus présentent selon nous des niveaux équivalents. Sur la question d'un refus de soin que pourrait engendrer un défaut d'identification, ce point est pour nous indépendant d'un choix de technologie de carte (cf. aspects déontologie ci-dessous).

- **Déontologie**

- ▶ **Conformément à l'article R.4235-61 du Code de la Santé Publique, lorsque l'intérêt de la santé du patient lui paraît l'exiger, le pharmacien doit refuser de dispenser un médicament.**
- ▶ **Si ce médicament est prescrit sur une ordonnance, le pharmacien doit informer immédiatement le prescripteur de son refus et le mentionner sur l'ordonnance.**

Faisabilité de la mise en place d'une carte vitale biométrique / aspects fraude à l'identité de l'assuré social et mesures envisageables pour un pharmacien lorsqu'il la détecte ou la soupçonne

- Le premier enjeu au niveau de l'impact d'une nouvelle génération de carte vitale pour le remboursement nous semble être celui du contrôle de l'ouverture des droits de la personne qui vient pour la dispensation de médicaments remboursés.
- Pour que cela se déroule correctement, les étapes principales nécessaires sont :
 - ▶ Que l'unicité du dispositif d'identification (carte ou appli) soit garantie ;
 - ▶ Qu'un téléservice de l'Assurance Maladie permette de vérifier en ligne le statut en termes de validité (non expiré et non révoqué) ou de forcer la mise à jour de la carte à intervalles réguliers ;
 - ▶ Qu'un téléservice de l'Assurance Maladie (le même que le précédent ou non) permette de vérifier l'ouverture des droits.
 - ▶ Nota : pour les deux derniers points ci-dessus, l'introduction de biométrie sur la carte vitale n'est pas un prérequis.
- Concernant la sécurisation renforcée de la prise en charge effective de la dispensation de médicaments sur ordonnance, ces étapes ci-dessus sont une condition nécessaire mais non suffisante. Ce qui permettra de boucler le dispositif sera le déploiement concomitant de deux autres services numériques :
 - ▶ L'identité numérique de santé (INS)
 - ▶ La e-prescription unifiée de médicaments pilotée par la CNAM
- **Pour nous c'est bien la conjonction de ces trois éléments, à savoir usage systématique de la e-prescription, inscription de l'INS dans la e-prescription et capacité de retrouver l'INS sur le dispositif d'identification présenté par le patient, qui rendra une fraude éventuelle beaucoup plus difficile à mettre en œuvre.**
- **Dans le cas où une anomalie serait détectée grâce aux moyens mis en œuvre, la principale question qui se poserait alors au niveau pratique est : quel accompagnement des pharmaciens en cas de doute ou de fraude avérée (collecte de données, signalement aux autorités compétentes) ?** Un accompagnement des pharmaciens doit en effet être prévu à l'instar de la procédure portant sur les médicaments onéreux.

Pièce jointe 4

**Courriel du directeur général de
la CNAM**

Courriel de M. Thomas Fatome, directeur général de la CNAM, à la mission IGAS-IGF, en date du 3 avril 2023

« Je tenais tout d'abord à vous remercier pour la qualité des échanges de vendredi. Suite à cette restitution, Il m'est apparu toutefois nécessaire de revenir vers vous à propos du projet de scénario d'un conteneur disposant du NIR dans la carte d'identité ou le titre de séjour électronique. En effet, il me semblait essentiel de vous faire part des très fortes réserves de l'Assurance maladie sur ce projet et de vous signaler tout l'intérêt qu'il y aurait à ce que cette position de l'assurance maladie figure explicitement dans votre rapport.

Premièrement, et dans l'exacte continuité des constats de la mission l'ayant conduit à rejeter le scénario de la CV biométrique, ce projet ne paraît répondre à aucun besoin :

1. sa plus-value en matière de LCF reste entièrement à démontrer à partir du moment où la mission considère que la notion de « fraude à la CV » n'est pas un concept opérant et que les montants de fraude susceptibles d'être liés à une utilisation frauduleuse de la carte vitale sont minimes ;
2. en outre, un tel projet ne permettrait pas non plus de répondre à un enjeu de simplification administrative dès lors que les professionnels de santé ne demandent pas aujourd'hui deux cartes (CV et CNI) à l'assuré mais bien une seule. Avec un tel scénario, aujourd'hui comme demain, les professionnels demanderaient 1 seul support au patient : la CV ou l'APCV aujourd'hui ; la CNIe avec le conteneur disposant du NIR demain.

Deuxièmement, une telle recommandation apparaît inopportune et pourrait fragiliser le déploiement de l'apCV, pourtant identifié par la mission comme un outil susceptible de palier certaines limites de la CV. Toute annonce relative au déploiement d'un nouvel outil alors que l'application est sur le point d'être lancée et que son usage reste encore à développer serait contre-productive et source d'incompréhension pour les assurés et les professionnels de santé.

Pour mémoire, nous allons prochainement débiter la phase de déploiement auprès d'un nombre limité d'assurés dans les 8 premiers départements pilotes. L'ouverture de l'application dans le store est prévue autour de la mi-mai pour un déploiement progressif durant une première phase pilote. Sous réserve des résultats de cette phase pilote, l'extension se ferait ensuite progressivement pas région à partir de septembre. Les mois à venir seront ainsi cruciaux pour la réussite de l'apCV et l'Assurance maladie (et le GIE) doivent travailler à l'accroissement de la notoriété de l'application auprès des PS et des assurés.

Dans un tel contexte, alors que la mission souligne elle-même que toute difficulté au moment du déploiement de l'apCV pourrait poser un problème d'image pour l'Assurance maladie et menacer durablement l'usage de l'application, il paraît incohérent de recommander en parallèle un scénario de développement d'une autre solution (y compris s'il s'agit uniquement d'investiguer dans les mois à venir un tel scénario).

Troisièmement, comme nous avons pu l'évoquer vendredi, une CNIe ou un titre de séjour électronique doté d'un conteneur supportant le NIR ne couvrirait pas couvrir l'ensemble de la population assurée, tant s'agissant notamment des ressortissants européens ou des assurés qui choisiraient de ne pas recourir à un tel conteneur disposant du NIR (condition de l'acceptation de la solution par la CNIL).

Ce scénario reviendrait ainsi à ajouter un support supplémentaire aux supports existants, qu'il ne pourra donc pas entièrement remplacer. Il n'y aurait pas, en contrepartie de la complexité accrue liée à ce nouveau support, plus de sécurisation lors de la facturation, puisqu'on aurait donc, des cartes Vitale physiques, des AP/CV, des CNI et toujours des personnes sans support.

Quatrièmement, on peut d'ores et déjà identifier un certain nombre de difficultés liées à un tel scénario.

3. *Au plan purement technique, l'inscription du NIR dans la CNIe suppose, outre la mise en œuvre d'échanges informatiques qui aujourd'hui n'existent pas, un alignement des trajectoires de délivrance, notamment en termes de délai. Par ailleurs, la notion d'inscription du NIR ne semble pas devoir être seule confondue avec celle de l'éligibilité de la personne à des prestations maladie (aujourd'hui les conditions d'octroi d'une carte Vitale, soit l'existence d'un NIR certifié/rattaché et d'un régime ouvert).*
4. *La possible dichotomie entre les droits à la prise en charge des frais de santé et la possibilité de solliciter une CNI ou un titre de séjours électroniques risque de poser des difficultés en termes de communication auprès des assurés, voire même des professionnels de santé qui solliciteraient la CNIe du patient mais ne pourraient rien en faire, faute de conteneur disposant du NIR.*
5. *Enfin, bien que la CNIL ne se soit pas opposée frontalement à ce scénario, elle a bien rappelé la question de la nécessaire proportionnalité entre la mise en place d'un tel outil et le besoin auquel il vise à répondre. Au-delà de cette question juridique, l'association sur un même support des données d'état civil et le NIR, même au sein de deux conteneurs distincts, risque d'être mal comprise, alors que les sphères « Intérieur » et « Sécurité sociale » étaient jusqu'ici strictement étanches. Le risque politique associé à un tel rapprochement, même si celui-ci est entouré de toutes les garanties possibles, ne doit pas être sous-estimé dans un contexte où le débat public sur ce type de sujets, alimenté par les fake news et les réseaux sociaux, peut très vite déraiser.*

S'il ressort clairement des conclusions de la mission que l'hypothèse d'une carte Vitale biométrique doit être écartée, cela ne saurait suffire à faire du scénario CNIe avec un conteneur disposant du NIR un scénario de repli légitime : ses avantages et ses inconvénients doivent, comme pour tout autre scénario, être soigneusement analysés. Pour l'Assurance maladie, en première analyse, il semble déjà assez clair que le rapport coûts / bénéfices d'un tel projet, tant en matière de mise en œuvre initiale qu'au travers des coûts de renouvellement pluriannuels, ne plaide pas en sa faveur. »

ANNEXE X

Liste des personnes rencontrées

SOMMAIRE

1. CABINETS MINISTÉRIELS	1
1.1. Cabinet du ministre de la santé et de la prévention	1
1.2. Cabinet du ministre délégué chargé des comptes publics	1
1.3. Cabinet de la ministre déléguée chargée de l'organisation territoriale et des professions de santé	1
2. ADMINISTRATIONS CENTRALES.....	1
2.1. Direction de la sécurité sociale.....	1
2.2. Direction générale de l'offre de soins	1
2.3. Direction des affaires juridiques des ministères chargés des affaires sociales.....	1
2.4. Délégation aux affaires européennes et internationales	2
2.5. Délégation ministérielle au numérique en santé.....	2
2.6. Direction du budget.....	2
2.7. Direction du management de l'administration territoriale et de l'encadrement supérieur	2
2.8. Mission interministérielle de coordination anti-fraude	2
2.9. Office centrale de lutte contre les atteintes à l'environnement et à la santé publique	3
2.10.. Office centrale de lutte contre le travail illégal.....	3
3. ORGANISMES DE SÉCURITÉ SOCIALE ET OPÉRATEURS ASSOCIÉS	3
3.1. Caisse nationale d'assurance maladie des travailleurs salariés	3
3.2. Caisse primaire d'assurance maladie des Alpes maritimes.....	4
3.3. Caisse primaire d'assurance maladie du Rhône.....	4
3.4. Caisse primaire d'assurance maladie de Seine-Saint-Denis	5
3.5. Caisse autonome nationale de la sécurité sociale du régime des Mines	5
3.6. Régime autonome de sécurité sociale du Sénat	5
3.7. GIE SESAM-Vitale	5
4. ORGANISMES REPRÉSENTATIFS DE L'ASSURANCE MALADIE COMPLÉMENTAIRE	5
4.1. Centre technique des institutions de prévoyance	5
4.2. Fédération nationale de la mutualité française	6
4.3. France Assureurs.....	6
5. OPÉRATEURS DE L'ÉTAT	6
5.1. Agence nationale de la sécurité des systèmes d'information	6
5.2. Agence nationale des titres sécurisés.....	6
6. ORDRES PROFESSIONNELS.....	6
6.1. Conseil national de l'ordre des infirmiers.....	6

6.2. Conseil national de l'ordre des médecins.....	6
6.3. Conseil national de l'ordre des pharmaciens.....	6
7. SYNDICATS DE PROFESSIONNELS LIBÉRAUX.....	7
7.1. Syndicats infirmiers	7
7.1.1. Fédération nationale des infirmiers	7
7.1.2. Syndicat national des infirmières et infirmiers libéraux.....	7
7.2. Syndicats représentatifs de médecins généralistes	7
7.2.1. Confédération des syndicats médicaux français	7
7.2.2. Fédération des médecins de France	7
7.2.3. Fédération française des médecins généralistes.....	7
7.2.4. Union française pour une médecine libre.....	7
7.3. Syndicats pharmaceutiques	8
7.3.1. Fédération des syndicats pharmaceutiques de France.....	8
7.3.2. Union syndicale des pharmaciens d'officine.....	8
8. ORGANISATIONS PROFESSIONNELLES D'ÉTABLISSEMENTS DE SANTÉ.....	8
8.1. Fédération des Établissements Hospitaliers et d'Aide à la Personne privés solidaires	8
8.2. Fédération hospitalière de France	8
8.3. Conférence des directeurs généraux de Centres hospitaliers universitaires.....	8
8.4. Fédération de l'hospitalisation privée.....	8
9. ETABLISSEMENTS DE SANTÉ	9
9.1. Assistance publique - Hôpitaux de Paris, groupe hospitalo-universitaire Paris Seine Saint Denis	9
9.2. Centre hospitalier de Perpignan	9
10. INDUSTRIELS DE LA BIOMÉTRIE	9
10.1. Idemia	9
10.2. IN Groupe	9
11. AUTRES ORGANISMES	10
11.1. CampusFrance.....	10
11.2. Commission nationale informatique et libertés.....	10
11.3. Cour des comptes.....	10
11.4. GIE Cartes bancaires	10
11.5. Institut national de la statistique et des études économiques	10
11.6. Union nationale des associations agréées d'usagers du système de santé	10
12. PERSONNALITÉS QUALIFIÉES.....	10

Annexe X

‡ signifie que l'ensemble des membres de la mission a effectué l'entretien en visioconférence ou en audioconférence.

1. Cabinets ministériels

1.1. Cabinet du ministre de la santé et de la prévention

M. Antoine MEFFRE, conseiller financement et protection sociale

1.2. Cabinet du ministre délégué chargé des comptes publics

M. Rayan NEZZAR, conseiller comptes et budgets sociaux

1.3. Cabinet de la ministre déléguée chargée de l'organisation territoriale et des professions de santé

M. Antoine-Mathieu NICOLI, directeur adjoint

M. Thibaut CHAIX‡, conseiller technique

2. Administrations centrales

2.1. Direction de la sécurité sociale

Mme Cristina CUENCA LÓPEZ, cheffe du bureau des systèmes d'information des organismes de sécurité sociale et réglementation des traitements de données à caractère personnel

M. François GODINEAU, expert de haut niveau

Mme Claire VINCENTI, sous-directrice du pilotage du service public de la sécurité sociale

2.2. Direction générale de l'offre de soins

Dr Gilles HEBBRECHT‡, adjoint à la cheffe du bureau système d'information des acteurs de l'offre de soins

Mme Cécile LAMBERT, cheffe de service

Mme Caroline LE GLOAN‡, cheffe du bureau système d'information des acteurs de l'offre de soins

2.3. Direction des affaires juridiques des ministères chargés des affaires sociales

M. Fabrice BRETÉCHÉ‡, sous-directeur de l'administration

M. Bastien BRILLET‡, sous-directeur des politiques

M. Émile GABRIÉ‡, chef du bureau du droit du numérique et des données

Annexe X

Mme Pearl NGUYÊN DUY‡, directrice

2.4. Délégation aux affaires européennes et internationales

Mme Catherine BORSI-SERHAN‡, responsable du pôle réseau des conseillers pour les affaires sociales

Mme Sarah CHERKAOUI‡, adjointe au conseiller pour les affaires sociales, ambassade de France à Stockholm

Mme Coralie GERVAISE‡, adjointe au conseiller pour les affaires sociales, ambassade de France à Londres

M. Pierre GOUDIN‡, conseiller pour les affaires sociales, ambassade de France à Rome

Mme Mireille JARRY‡, conseillère pour les affaires sociales, ambassade de France à Madrid

Mme Marguerite MOLEUX‡, conseillère pour les affaires sociales, ambassade de France à Londres

M. Pierre PERARD‡, adjoint au conseiller pour les affaires sociales de Stockholm, ambassade de France à Copenhague

M. Benoit SEVCIK‡, conseiller pour les affaires sociales, ambassade de France à Washington

M. Jean THIEBAUD‡, chef de cabinet

2.5. Délégation ministérielle au numérique en santé

M. Raphaël BEAUFRET‡, directeur de projet-responsable du numérique en santé

2.6. Direction du budget

Mme Marie CHANCHOLE, sous-directrice de la 6^{ème} sous-direction

M. John HOULDSWORTH, adjoint à la sous-directrice de la 6^{ème} sous-direction

M. Laurent PELLEN, chef du bureau des comptes sociaux

2.7. Direction du management de l'administration territoriale et de l'encadrement supérieur

M. Jonathan BLOCH, adjoint à la mission transformation numérique

Mme Emmanuelle FRESNAY, adjointe à la cheffe de la mission ministérielle la lutte contre la fraude documentaire et à l'identité

Mme Virginie GUERIN-ROBINET, cheffe de la mission ministérielle la lutte contre la fraude documentaire et à l'identité

2.8. Mission interministérielle de coordination anti-fraude

M. Éric BELFAYOL, chef de la mission

M. Yann PORTAT, chef du projet enjeux sociaux

2.9. Office centrale de lutte contre les atteintes à l'environnement et à la santé publique

Dr Fabienne HELLER-BONOMI‡, conseillère santé

LCL Sébastien NOCHEZ‡, chef de la division stratégie analyse

GBR Sylvain NOYAU‡, commandant de l'OCLAESP

2.10. Office centrale de lutte contre le travail illégal

CNE Olivier BROGGI, commandement du groupe fraude aux prestations sociales

COL Paul CHAUDANSON, commandant en second de l'OCLTI

LCL Cécile LAMBERT, bureau criminalité organisée et délinquance spécialisée (sous-direction de la police judiciaire de la Direction générale de la gendarmerie nationale)

GBR Dominique LAMBERT, commandant l'OCLTI

CNE Stéphane SABOTIER, commandant de la division investigation

3. Organismes de sécurité sociale et opérateurs associés

3.1. Caisse nationale d'assurance maladie des travailleurs salariés

Mme Vanessa AUDEBERT, chargée de missions, département juridique

M. Fabien BADINIER, directeur adjoint, direction déléguée de l'audit, des finances et de la lutte contre la fraude

Mme Christel BENDEL-SCHMID, chargée de mission, département Sésam-Vitale, direction déléguée à la gestion et à l'organisation des soins

Mme Bintou BOÏTÉ‡, responsable maîtrise d'ouvrage, direction déléguée aux opérations

Mme Manon CHONAVEL, directrice de cabinet

Mme Gildine CROIZÉ, responsable du département juridique, déléguée à la protection des données

Mme Elisabeth DEMUS, Responsable du département prévention, maîtrise des risques et réglementation financière, direction déléguée de l'audit, des finances et de la lutte contre la fraude

M. Nicolas DENIS, responsable maîtrise d'ouvrage carte Vitale, direction déléguée aux opérations

M. Emmanuel GOMEZ, directeur de la maîtrise d'ouvrage tarification, rémunération, application carte Vitale, prévention, direction déléguée à la gestion et à l'organisation des soins

M. Thomas FATOME‡, directeur général

Mme Sara-Lou GERBER‡, directrice de cabinet

Mme Anne-Louise HAUTEFORT, chargée de missions, département juridique

Mme Isabelle IEM‡, responsable maîtrise d'ouvrage carte Vitale, direction déléguée aux opérations

Annexe X

M. Alexandre LECORRE, responsable adjoint du département investigation ville et accès aux droits, direction déléguée de l'audit, des finances et de la lutte contre la fraude

Mme Audrey PALMENTIER, chargée de missions conformité, département juridique

M. Pierre PEIX, directeur, direction déléguée aux opérations

M. Pierig POULIQUEN‡, responsable de la mission d'accompagnement des régimes partenaires, direction déléguée aux opérations

Mme Ingrid RICHARD, attachée de direction, direction déléguée de l'audit, des finances et de la lutte contre la fraude

M. Jérôme RODENBACH, responsable du département droit des contentieux, direction déléguée de l'audit, des finances et de la lutte contre la fraude

Mme Sophie SCHNEIDER‡, chargée des cartes Vitale, mission d'accompagnement des régimes partenaires, direction déléguée aux opérations

M. Marc SCHOLLER, directeur, direction déléguée de l'audit, des finances et de la lutte contre la fraude

M. Simon VOILLET, chargé des relations avec les corps de contrôle, direction déléguée aux opérations

M. Nicolas VOIRIN, responsable du département efficience, direction déléguée de l'audit, des finances et de la lutte contre la fraude

3.2. Caisse primaire d'assurance maladie des Alpes maritimes

Mme Sophie BIAMONTI‡, pilote gestion des bénéficiaires

Mme Sophie PIZARRO‡, copilote gestion des bénéficiaires

Mme Nathalie MARTIN‡, directrice

Mme Gwenaëlle TASSET‡, sous-directrice santé et prestations sociales

Mme Élodie TOURNAY‡, responsable accompagnement des offreurs de soins et pilote de l'expérimentation ApCV pour les Alpes maritimes

3.3. Caisse primaire d'assurance maladie du Rhône

Mme Magali CARDI‡, chargée de mission auprès de la direction de la maîtrise des dépenses de santé

Mme Estelle COULET‡, sous directrice en charge de la direction de la maîtrise des dépenses de santé

Mme Camille DROUIN‡, stagiaire de l'école nationale supérieure de la sécurité sociale

Mme Laurence GAMET‡, responsable du cabinet de la direction générale

Mme Astrid GAUGY‡, responsable adjointe du service de lutte contre les fraudes

M. Dominique GRANJON‡, responsable du département frais de santé

M. Grégory MARTEL‡, responsable du service contrôle

M. Mathieu MARTINEZ‡, responsable du service conseillers informatique service

M. Yassine NECHADI‡, responsable du département gestion des bénéficiaires

M. Guillaume PRATO‡, directeur adjoint en charge des relations et services aux clients

3.4. Caisse primaire d'assurance maladie de Seine-Saint-Denis

Audrey ARBONA-PAUPY, responsable du département lutte contre les fraudes

M. Willi CANTIE, délégué numérique en santé

Mme Aurélie COMBAS-RICHARD, directrice générale

M. Ahmed KADI, délégué numérique en santé

Mme Marie LAFAGE, directrice de la santé et des affaires juridiques

Mme Gianfranca LEFEBVRE, responsable du département gestion des droits

M. Jean-Gabriel MOURAUD, directeur général adjoint

Mme Cathy RICHARDSON, responsable du service frais de santé

3.5. Caisse autonome nationale de la sécurité sociale du régime des Mines

M. Olivier AUBRY‡, directeur national du budget et des gestions assurantielles

3.6. Régime autonome de sécurité sociale du Sénat

M. Vincent DELSART, directeur des affaires financières et sociales

M. Jean GUISELIN, responsable de la division de la protection sociale

Mme Yvelise LAPASIN, responsable du pôle affiliation

3.7. GIE SESAM-Vitale

M. Philippe BRIENT, directeur de la transformation, de l'expertise et du pilotage

M. Benoit CALMELS, responsable sécurité des systèmes d'information

M. Jean-Luc DAUVOIS, directeur de projets domaine cartes

M. Dominique DE RAIGNIAC, directeur de projets domaine mise à jour cartes

M. Anthony GOMES DE CARVALHO, directeur général

M. Sébastien HOUGET, directeur de projets domaine facturation

M. Frédéric PICARD, directeur de projets domaine appli carte vitale (ApCV)

M. Jean-Marc VAN BINNEVELD, responsable marchés production cartes

M. Michel VENET, directeur de l'identité numérique

M. Olivier VILLETTE, architecte système

4. Organismes représentatifs de l'assurance maladie complémentaire

4.1. Centre technique des institutions de prévoyance

M. Philippe DABAT‡, vice-président inter AMC

Mme Morgane LANGLOIS-GAUTIER‡, responsable pôle systèmes d'information en santé

4.2. Fédération nationale de la mutualité française

M. Christophe LAPIERRE‡, responsable systèmes d'information de santé

Mme Françoise GIRAUT‡, adjointe au responsable systèmes d'information de santé

4.3. France Assureurs

M. Pierre FRANÇOIS‡, commission santé

Mme Nathalie STEL‡, sous-directrice systèmes d'information santé et collectives

5. Opérateurs de l'État

5.1. Agence nationale de la sécurité des systèmes d'information

Mme Aline GOUGET MORIN‡, cheffe adjointe de la division scientifique et technique, sous-direction expertise

Renaud LABELLE‡, sous-directeur expertise

5.2. Agence nationale des titres sécurisés

Mme Anne-Gaëlle BAUDOUIIN, directrice

M. Pierre ORSZAG, responsable des titres sécurisés

M. Florent TOURNOIS‡, directeur du programme identité numérique

M. Jean-Karim ZINZINDOHOUE, directeur technique du programme identité numérique

6. Ordres professionnels

6.1. Conseil national de l'ordre des infirmiers

M. Patrick CHAMBOREDON‡, président

6.2. Conseil national de l'ordre des médecins

Dr Catherine GUINTOLI-CENTURI‡, Vice-président de la section exercice professionnel

Dr René-Pierre LABARRIÈRE, président de la section exercice professionnel

Pr Stéphane OUSTRIC‡, médecin généraliste, délégué général aux données de santé et au numérique, président du conseil départemental de l'ordre des médecins de Haute-Garonne

Mme Marine THOMASSIN, conseiller juridique

6.3. Conseil national de l'ordre des pharmaciens

Mme Caroline LHOPITEAU‡, directrice générale

Annexe X

Dr Patrick MAZAUD‡, élu section H

Mme Véronique PERRIN‡, directrice de l'exercice professionnel

M. Olivier PORTE‡, directeur des technologies en santé

Dr Carine WOLF-THAL‡, présidente

7. Syndicats de professionnels libéraux

7.1. Syndicats infirmiers

7.1.1. Fédération nationale des infirmiers

M. Julien BOEHRINGER‡, vice-président délégué

M. Daniel GUILLERM‡, président

Mme Pascale LEJEUNE‡, secrétaire générale

7.1.2. Syndicat national des infirmières et infirmiers libéraux

M. John PINTE‡, président

7.2. Syndicats représentatifs de médecins généralistes

7.2.1. Confédération des syndicats médicaux français

Dr Franck DEVULDER‡, président

7.2.2. Fédération des médecins de France

Dr Pascal CHARBONNEL‡, médecin généraliste

Dr Corinne LE SAUDER‡, présidente

7.2.3. Fédération française des médecins généralistes

Dr Gilles URBEJTEL‡, conseiller du bureau national

7.2.4. Union française pour une médecine libre

Dr Jérôme MARTY‡, président

7.3. Syndicats pharmaceutiques

7.3.1. Fédération des syndicats pharmaceutiques de France

Dr Philippe BESSET‡, président

Mme Mahé CAUCHARD‡, juriste

M. Pierre FERNANDEZ‡, directeur général

Dr Valérian PONSINET‡, président de la commission convention et systèmes d'information

7.3.2. Union syndicale des pharmaciens d'officine

Dr Pierre-Olivier VARIOT‡, président

Dr Sébastien LAGOUTTE‡, membre du bureau national chargé du numérique

8. Organisations professionnelles d'établissements de santé

8.1. Fédération des Établissements Hospitaliers et d'Aide à la Personne privés solidaires

M. Laurent PIERRE‡, conseiller numérique

8.2. Fédération hospitalière de France

M. Aurélien SOURDILLE‡, responsable adjoint du pôle offre

8.3. Conférence des directeurs généraux de Centres hospitaliers universitaires

M. Olivier BOSSARD‡, directeur général du CHU de Saint-Étienne

M. Vincent DUPONT‡, directeur coordonnateur du pôle efficience, finances et qualité du CHU d'Amiens-Picardie

M. Francis KRAUSE‡, directeur adjoint du pôle efficience, finances et qualité du CHU d'Amiens-Picardie

M. Nicolas MEYNIEL‡, directeur des affaires financières et du contrôle de gestion du CHU de Saint-Étienne

Mme Danielle PORTAL‡, directrice générale du CHU d'Amiens-Picardie

M. Lucas TIDADINI‡, directeur adjoint des finances, CHU de Reims

8.4. Fédération de l'hospitalisation privée

M. Bertrand SOMMIER‡, secrétaire général, chargé des dossiers numériques

Mme Marie-Claire VIEZ‡, directrice de la stratégie

9. Établissements de santé

9.1. Assistance publique - Hôpitaux de Paris, groupe hospitalo-universitaire Paris Seine Saint Denis

Mme Amélie CANTAT, Directrice adjointe des finances

M. Jean-Bernard LAHANAL‡, cadre de santé, service des urgences

M. Jérôme VANTORHOUDT, Responsable des admissions – frais de séjour et traitements externes

9.2. Centre hospitalier de Perpignan

Dr Éric BORDART‡, chef de service du département de l'information médicale et référent en identitovigilance

Mme Céline BRIGNON-DAVID‡, responsable du bureau des admissions/facturation

Mme Sylvie CARRÈRE‡, cadre supérieur de santé (pôle des urgences)

M. Grégory GUIBERT‡, directeur administratif et financier

Mme Emmanuelle LANDREAU‡, responsable de la cellule d'identitovigilance opérationnelle

M. Barthélémy MAYOL‡, directeur

Mme Véronique SAUNIER‡, cadre assistant sociaux éducatifs

10. Industriels de la biométrie

10.1. Idemia

M. Emmanuel CARLE, chef de programme identité et sécurité publique

Mme Véronique MENARD-ROPP, responsable relation commerciale identité et sécurité publique

M. Laurent PELLEGRIN, directeur France identité et sécurité publique

10.2. IN Groupe

M. David CONCORDEL, vice-président, responsable du pôle services digitaux

M. Romain GALESNE-FONTAINE, directeur de la communication et des relations institutionnelles

M. Yann HAGUET, vice-président, responsable du pôle identité

M. Audrey MARIANI, secrétaire générale

Mme Carole PELEGRINO, déléguée à la protection des données

M. Pierre WARNEZ, directeur des activités cartes et passeports

11. Autres organismes

11.1. CampusFrance

M. Patrice GOUJET‡, chargé de mission

Mme Donatienne HISSARD‡, directrice générale

Mme Karine MOUCHELIN‡, directrice adjointe de l'accueil et de la vie étudiante

M. Guillaume TÉTARD‡, chargé d'études statistiques

11.2. Commission nationale informatique et libertés

Mme Inès BEDAR, juriste, service des affaires régaliennes et des collectivités locales

M. Erik BOUCHER DE CREVECOEUR, ingénieur expert, service de l'expertise technologique

M. Thomas DAUTIEU, directeur de l'accompagnement juridique

Mme Aurore GIGNON, juriste, service de la santé

Mme Hélène GUIMIOT-BREAUD‡, cheffe du service de la santé

M. Félicien VALLET‡, chef adjoint du service de l'expertise technologique

11.3. Cour des comptes

Mme Véronique HAMAYON, présidente de la 6^{ème} chambre

M. Jean-Pierre VIOLA, président de section au sein de la 6^{ème} chambre

11.4. GIE Cartes bancaires

M. Philippe LAULANIE, administrateur

M. Loÿs MOULIN, directeur du développement

11.5. Institut national de la statistique et des études économiques

Mme Muriel BARLET‡, cheffe du département démographie

M. Lionel ESPINASSE‡, adjoint à la cheffe du département démographie

11.6. Union nationale des associations agréées d'usagers du système de santé

Mme Féreuze AZIZA, chargée de mission assurance maladie

M. Arthur DAUPHIN, chargé de mission numérique en santé

12. Personnalités qualifiées

Dr Sylvie BAQUÉ‡, inspectrice générale des affaires sociales en service extraordinaire, ancienne présidente de la Commission médicale d'établissement du Centre hospitalier Ariège-Couserans

Annexe X

M. Pierre BOURGEOIS, inspecteur général de l'administration, membre de la mission d'expertise et de contrôle en matière de délivrance des titres réglementaires

Dr Manuela OLIVER‡, groupe régional d'identitovigilance des établissements de santé (PACA), référent régional

Mme Valérie PÉNEAU‡, ancienne directrice du programme interministériel France Identité Numérique

M. Frédéric PICHON‡, inspecteur général de l'administration, ancien adjoint à la directrice du programme interministériel France Identité Numérique

M. Philippe SUDREAU‡, inspecteur général des affaires sociales, ancien directeur général du CHU de Nantes

PIÈCE JOINTE

Lettre de mission



GOVERNEMENT

Liberté
Égalité
Fraternité

Les Ministres

Paris, le 18 OCT. 2022

NOTE

A

Madame la cheffe du service de l'inspection générale des finances,

Monsieur le chef du service de l'inspection générale des affaires sociales

Objet : Mise en place d'une carte Vitale biométrique

La création d'une carte vitale biométrique, évoquée à de nombreuses reprises ces dernières années pour lutter contre la fraude à l'utilisation par des tiers non assurés sociaux ou par des assurés voulant bénéficier d'une meilleure couverture des dépenses (exonérations de participation ou complémentaire santé solidaire), a donné lieu à plusieurs initiatives parlementaires. Récemment, la loi de finances rectificative (LFR) n° 2022-1157 du 16 août 2022 a ouvert une enveloppe de 20 millions d'euros au sein de la mission « Santé » afin de lancer le chantier de la carte Vitale biométrique.

Dans ce contexte, nous souhaitons qu'une mission soit conduite pour évaluer la pertinence et l'intérêt de mettre en place une carte biométrique au vu des enjeux de lutte contre la fraude sociale mis en avant pour en justifier le déploiement à tous les assurés sociaux.

En premier lieu, la mission réalisera un recensement des travaux déjà conduits ou accomplis pour évaluer la fraude liée à l'usage des cartes afin de déterminer la portée d'une telle fraude, son origine et les modes d'organisation associés, sa volumétrie ainsi que son impact financier (s'agissant notamment des personnes n'ayant droit à aucune couverture sociale, ni à la protection maladie universelle ni à l'aide médicale d'Etat). En l'absence d'éléments tangibles, il conviendra de préciser la méthodologie susceptible d'apporter des éléments nouveaux. La mission appréciera également l'impact des mesures prises et des actions menées depuis 2004 pour réduire les risques liés à la délivrance de la carte et sécuriser le système d'émission et de blocage ou destruction des cartes ainsi que les facturations.

En second lieu, la mission analysera les différentes solutions techniques qui pourraient être utilisées aux fins d'en documenter la faisabilité et les changements qui découleraient de l'adoption de ces solutions. Pour mémoire, l'expérimentation en cours de l'application carte Vitale (e-carte Vitale ou ApCV) intègre, pour sécuriser l'identification de la personne, de la biométrie. Au vu des travaux techniques conduits et des résultats de l'expérimentation en cours, la mission pourra proposer les mesures qui seraient susceptibles d'accélérer et de faciliter le déploiement de l'application et son utilisation.

En troisième lieu, la mission s'intéressera aux conditions le cas échéant de déploiement de ces outils ainsi qu'à leurs coûts de mise en œuvre, aussi bien auprès des établissements de santé, des centres de santé qu'auprès des praticiens libéraux dans l'hypothèse d'un recours à la biométrie pour l'activation de la carte vitale dans le parcours de soins.

.../...

Les évolutions récentes ont amélioré les outils mis à disposition des professionnels et établissements qui disposent des droits en ligne et peuvent facilement vérifier la situation des droits de l'assuré. L'ajout d'une étape préalable d'identification biométrique peut être un facteur de complexité du processus, pour un intérêt qui doit être objectivé, au regard notamment de la fiabilité des différentes méthodes d'identification et du délai de mise en place d'une telle solution. La mission précisera donc les avantages pouvant être attendus de l'utilisation de la carte vitale biométrique pour lutter contre la fraude sociale, ainsi que les possibles impacts qui pourraient résulter du recours à l'activation de la carte par la biométrie lors de chaque facturation de soins.

La mission devra en outre, en lien avec la direction des affaires juridiques (DAJ) des ministères sociaux, conduire une analyse des questions juridiques qui seraient soulevées par le déploiement d'un tel dispositif, notamment le respect du RGPD, des principes de respect de la vie privée et des libertés publiques et les réponses qu'il serait nécessaire d'apporter. Elle prendra également contact avec la CNIL pour recueillir son appréciation sur la mise en place d'un tel dispositif.

Enfin, au regard des analyses menées, **la mission consultera les représentants des patients, les représentants des professionnels et des établissements et centres de santé**, de façon à apprécier les conditions de mise en œuvre de la ou des solutions préconisées.

Votre rapport devra être remis au plus tard à la fin du mois de janvier 2023.



François BRAUN
Ministre de la Santé et de la Prévention



Gabriel ATTAL
Ministre délégué chargé des Comptes publics