Movebook

IA et fraude en assurance santé : vigile ou complice ?

PRÉFACE

La fraude à l'assurance santé n'est plus un phénomène marginal : en 2025, elle constitue l'un des risques qui pèsent sur la soutenabilité de notre système de santé. Estimée à près de 4 milliards d'Euros par an, elle fragilise non seulement l'équilibre financier du secteur, mais aussi la confiance, par exemple, entre soignants, assureurs et assurés.
Face à ce défi, les acteurs du secteur de l'assurance n'ont pas le choix : ils doivent réinventer leur manière de détecter, comprendre et contrer ces pratiques. Et l'arme la plus prometteuse s'appelle… l'intelligence artificielle. Capable de traiter des millions de données en temps réel, de révéler des signaux faibles invisibles à l'œil humain et d'anticiper les schémas frauduleux, l'IA redéfinit déjà les contours de la lutte antifraude. Mais elle pose aussi une question centrale : jusqu'où peut-on déléguer la vigilance à la machine, sans perdre la confiance et l'équité qui fondent l'assurance santé ?

Ce MoveBook n'est ni un manuel technique, ni un rapport d'experts. C'est un cahier de tendances, proposé par Vovoxx Média, pensé pour éclairer les professionnels de l'assurance sur ce sujet majeur. Vous y trouverez des chiffres, des analyses, des témoignages et des pistes d'action qui dessinent le futur proche : celui d'une lutte antifraude où la technologie ne remplace pas l'humain, mais l'augmente ; où l'éthique et la transparence deviennent aussi importantes que la performance ; où la coopération pourrait, probablement faire la différence.

L'IA ne résoudra pas tout. Mais elle ouvre une nouvelle page dans le combat contre la fraude en santé. Ce MoveBook vous propose d'en explorer les lignes de force, les paradoxes et les opportunités. À vous, professionnels de l'assurance, de transformer ces perspectives en leviers concrets.

Nous remercions de leurs contributions : Cyrille Isaac-Sibille - Député, Maxence Bizien - ALFA, David Dumas-Lattaque - Shift Technology, Yann Abeloos - CEGEDIM Assurances et les 102 professionnels de l'assurance qui ont répondu à notre enquête.

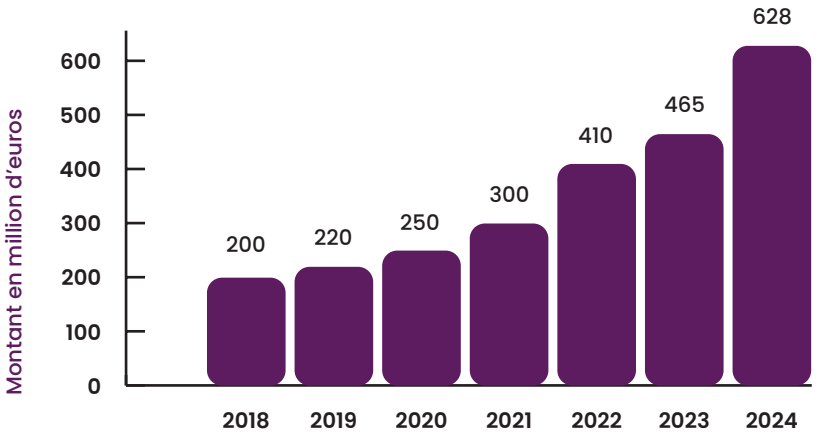
Jean-Luc Gambey
Directeur des publications et Associé
Vovoxx Média

SOMMAIRE

Contexte général

La fraude à l'assurance santé est devenue, en 2025, l'un des enjeux majeurs pour le système de santé français. Longtemps perçue comme marginale, elle atteint désormais des proportions critiques. Selon la Caisse Nationale d'Assurance Maladie (CNAM), **628 M€ de fraudes ont été détectés en 2024**, soit une hausse de +35 % par rapport à 2023 (Ameli).

Evolution des fraudes détectées par l'Assurance Maladie (2018-2024)



Mais les estimations globales situent le montant réel de la fraude autour de 4 Md€ par an (Cour des comptes). Cette dynamique s'explique par trois tendances majeures :

• **La dématérialisation accélérée du parcours de soins :** généralisation du tiers payant, essor des téléconsultations (plus de 11,6 M€ en 2023, dont 5,5 M€ en médecine générale), ordonnances électroniques et développement des objets connectés de santé.

• **La valeur croissante des données de santé :** considérées comme encore plus sensibles que les données bancaires, elles alimentent un marché noir en pleine expansion. En 2024, la CNIL a été notifiée de 5 629 violations de données personnelles, soit une progression de +20 % par rapport à 2023, confirmant l'attractivité de ces données pour les cybercriminels (CNIL)

• **La sophistication des fraudeurs :** ordonnances falsifiées, surfacturations abusives dans certains centres de santé, usurpations massives d'identité et fraudes liées aux équipements médicaux, comme les audioprothèses (plus de 115 M€ détectés en 2024) (Ameli).

CHIFFRES CLÉS À RETENIR

628 M€
de fraudes détectées en 2024
(+35 % en un an)

≈ 4 Md€
estimés de fraudes par an

5 629 violations de données personnelles
notifiées en 2024 (+20 % vs 2023)

Les professionnels de santé concentrent près de 70 %
des montants frauduleux détectés (Ameli).

1. LA FRAUDE SANTÉ : DE QUOI PARLE-T-ON ?

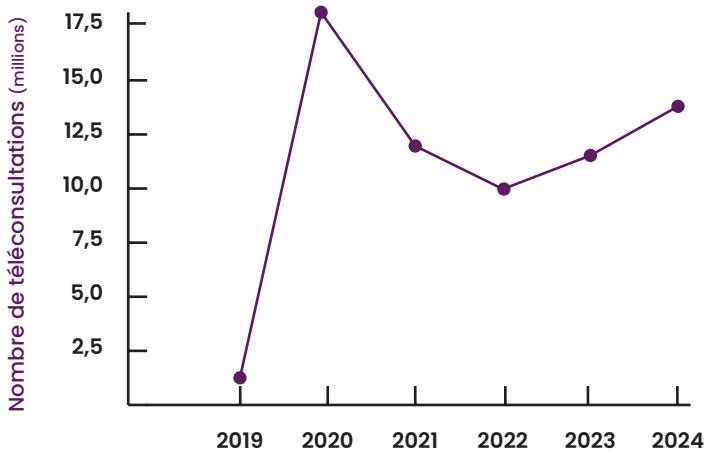
En 2025, la fraude en santé s'impose comme un défi majeur pour l'Assurance Maladie et les complémentaires santé. Longtemps perçue comme marginale, elle atteint désormais des proportions préoccupantes, nourrie par la dématérialisation accélérée du parcours de soins, la massification des données de santé et la sophistication croissante des réseaux frauduleux.

Dès lors, les schémas frauduleux sont multiples : actes fictifs, ordonnances falsifiées, surfacturations, usurpations d'identité, mais aussi fuites massives de données de santé exploitées à des fins frauduleuses. La fraude santé combine à la fois des comportements **opportunistes** (fraude individuelle) et des logiques **structurées/organisées** s'appuyant sur des réseaux professionnels ou des cyberattaques sophistiquées.

Explosion des données de santé

La transition numérique du secteur santé a entraîné une croissance massive des données produites. Les téléconsultations, par exemple, ont atteint, selon la Cour des comptes, un pic de 18 millions en 2020, avant de revenir à 11,6 millions en 2023 (dont 5,5 M€ réalisées en médecine générale). En 2024, leur nombre est reparti à la hausse pour atteindre 13,9 millions d'actes (Ameli).

Téléconsultation en France (2019-2024)



Source : Cour des comptes / Ameli

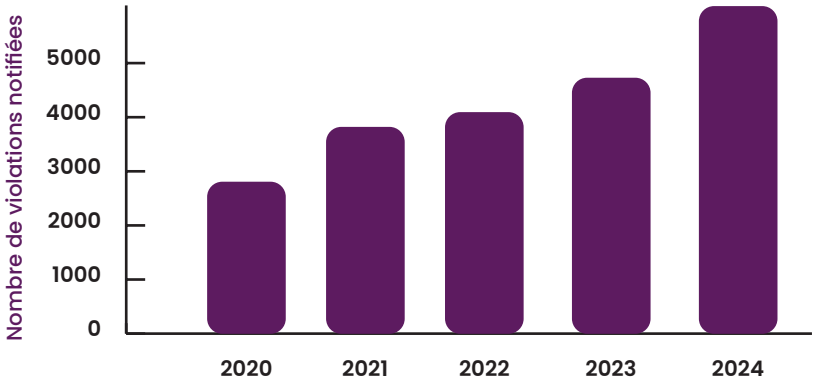
Parallèlement, la pratique du **tiers payant** s'est généralisée, progressant de plus de 5 points entre 2020 et 2023 (selon Viamedis). Le **Système National des Données de Santé (SNDS)** continue quant à lui de s'enrichir chaque année avec des informations relatives aux prescriptions, aux coûts et à la démographie des patients, notamment grâce aux objets connectés santé, qui multiplient les points de vulnérabilité.

Cette abondance de données améliore la coordination médicale et l'accès aux soins, mais ouvre aussi de nouvelles portes à la fraude : dossiers fictifs, usurpations d'identité, surfacturations difficiles à détecter à grande échelle.

Fuites et cyberattaques sur les données de santé

Les données de santé sont devenues une cible privilégiée pour les cybercriminels, car elles valent davantage que des données bancaires. En **2023, 4 668 fuites de données** ont été notifiées en France, soit environ 13 incidents par jour, représentant une hausse de +16 % par rapport à 2022. En **2024**, la CNIL a été notifiée de **5 629 violations de données personnelles**, soit une progression de **+20 % par rapport à 2023** (CNIL).

Fuite de données de santé déclarés en France (2020-2024)



Source : CNIL

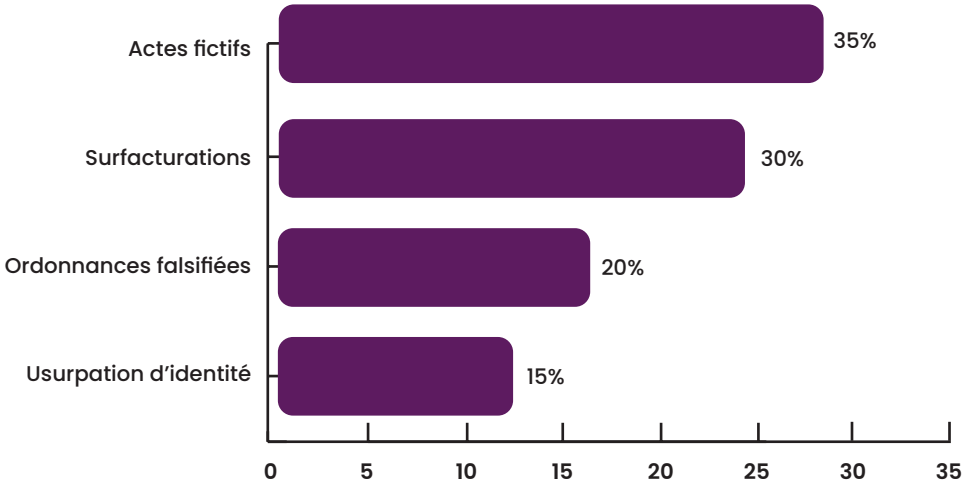
Même les infrastructures publiques ne sont pas épargnées : en 2022, la CNAM a subi une cyberattaque exposant les données personnelles de **510 000 assurés** (Ameli). Ces failles alimentent directement les fraudes (actes fictifs, ordonnances falsifiées, remboursements indus) et fragilisent la confiance des assurés.

Typologies de fraudes

Les pratiques frauduleuses détectées couvrent un spectre large, par exemples :

- **Actes fictifs** (ex : téléconsultations facturées sans avoir eu lieu, ….),
- **Surfacturations abusives**, notamment pour l'optiques et le dentaire,
- **Usurpations d'identité et dossiers falsifiés**,
- **Ordonnances contrefaites**, de plus en plus souvent générées via des outils numériques.

Répartition des typologie de fraudes santé (2024)



Source : Ameli

En 2024, plusieurs affaires ont marqué l'actualité : sept centres de santé ont été déconventionnés pour un préjudice estimé selon certaines sources de **6,6 M€**, tandis que la fraude aux audioprothèses a été multipliée par cinq en un an, atteignant **115 M€ détectés** (Ameli). Près de **68 % du montant total des fraudes détectées proviennent directement de professionnels de santé** (infirmiers, audioprothésistes, pharmaciens, centres de soins), ce qui souligne l'ampleur du défi dans la relation entre assureurs et praticiens (Ameli).

Un cadre réglementaire renforcé

Pour répondre à cette menace, le cadre juridique a été considérablement renforcé.

- Le **Règlement Général sur la Protection des Données (RGPD)** impose la notification des violations dans un délai de 72 h et prévoit des sanctions pouvant atteindre plusieurs millions d'Euros. En 2024, la CNIL a prononcé **87 sanctions et 180 mises en demeure**, pour un montant total de **55,2 M€** ; Certaines décisions ont marqué les esprits, avec des amendes significatives infligées à des acteurs de la santé pour traitement illicite de données médicales.
- Certaines décisions ont marqué les esprits. En 2024, la CNIL a infligé une amende de **800 000 € à un acteur de l'assurance santé** pour traitement illicite de données médicales, rappelant l'importance de la conformité en matière de protection des données.
- L'**IA Act**, entré en vigueur en août 2024, classe les systèmes d'intelligence artificielle appliqués à la santé comme des applications à haut risque, imposant des garanties strictes en matière de transparence, supervision humaine et auditabilité.
- L'**European Health Data Space** (EHDS), instauré en mars 2025, favorise l'interopérabilité et la gouvernance commune des données au niveau européen.

Une matrice complexe et fragile

La fraude santé en 2025 combine une **infrastructure numérique croissante** et des **vulnérabilités persistantes**. Si la dématérialisation a permis d'améliorer l'accès aux soins et la fluidité du parcours patient, elle a également ouvert la voie à des fraudes de plus en plus sophistiquées. Les fraudeurs exploitent à la fois les failles techniques, la valeur des données sensibles et les limites des contrôles traditionnels.
Dans ce contexte, l'innovation technologique et l'intelligence artificielle apparaissent comme des leviers stratégiques pour renforcer la détection, anticiper les menaces et restaurer la confiance entre acteurs du système de santé.

CHIFFRES CLÉS À RETENIR

- 18 Millions de téléconsultations en 2020, contre 11,6 Millions en 2023 et **13,9 Millions en 2024**
- **+5 points de progression du tiers payant entre 2020 et 2023**
- **510 000 assurés impactés** par une cyberattaque contre la CNAM en 2022
- 7 centres de santé déconventionnés en 2024 pour un **préjudice de 6,6 M€**
- **115 M€ de fraudes détectées** sur les audioprothèses en 2024 (×5 en un an)
- **68 % du montant des fraudes détectées** proviennent de professionnels de santé
- En 2024, la CNIL a prononcé **87 sanctions et 180 mises en demeure, pour un total de 55,2 M€**

Maxence Bizien
est Directeur général de l'ALFA (Agence de Lutte contre la Fraude à l'Assurance), association affiliée à France Assureurs. Son interview a été réalisée le 17/09/2025.

Comment L'ALFA[1] voit-elle l'évolution de la fraude sur le périmètre de l'assurance santé, de la prévoyance ?

La fraude dans le domaine de la santé représenterait plusieurs milliards d'Euros pour l'ensemble des acteurs publics et privés. Bien que de nombreuses études ont été menées sur le sujet, les différents acteurs peinent encore à s'accorder sur les enjeux. Dans son rapport de 2020 intitulé « La lutte contre les fraudes aux prestations sociales, la Cour des comptes indiquait ne pas être en mesure d'estimer avec précision les montants concernés, évaluant toutefois la fraude potentielle à environ 14 milliards d'Euros. Cette même institution constatait que les progrès réalisés étaient trop lents et qu'un changement d'échelle était donc indispensable. Depuis lors, la Sécurité Sociale a poursuivi son travail sur ce sujet, estimant que le taux de fraude variait entre 3 % et 7 % selon la nature des dépenses.

Sur la branche maladie, si l'on considère un taux de fraude à 5% sur les 226 milliards d'Euros de prestations nettes versées en 2023, l'enjeu s'élève à 11,3 milliards d'Euros.

Pour les organismes complémentaires, aucune étude scientifique ou actuarielle formelle n'a été menée par des centres de recherche en France. Certains pays, plutôt anglo-saxons, ont essayé d'évaluer la fraude dans ce domaine. À partir de quelques éléments de comparaison sur nos portefeuilles, côté organismes d'assurance santé nous arriverions à un enjeu de 2,7 milliards d'Euros. Le potentiel d'économie pour le secteur est majeur, sachant qu'il faut distinguer la fraude réelle de ce que l'on peut réellement identifier. C'est un leurre de croire que nous pourrons endiguer la totalité de la fraude en assurance santé.
Concernant l'Assurance maladie, 628 millions d'Euros de fraudes ont été identifiés en 2024. Mais cela ne veut pas dire que l'intégralité des fraudes ont été stoppées : le montant réellement empêché reste inférieur. Chaque année l'ALFA

demande à ses plus de 345 adhérents un reporting de leurs activités de lutte contre la fraude. C'est une démarche volontaire de leur part. Les organismes d'assurance santé et les acteurs de l'assurance IARD participent activement à cette collecte de données chiffrées. Côté santé prévoyance, le reporting à l'ALFA est beaucoup plus récent. Si le sujet de la fraude a été longtemps tabou, la fraude santé s'est révélée au grand jour avec le 100% santé. En matière de fraude, il y a une règle : on ne la voit que si on la cherche. Une fois détectée, il est essentiel de s'appliquer à l'enregistrer et à transmettre cette comptabilisation à l'ALFA, si l'on est adhérent. En 2023, au niveau global nous avons comptabilisé 695 millions d'Euros de fraude identifiés (IARD, Santé, Prévoyance, assurance vie), dont 485 millions d'Euros en IARD et 83 millions d'Euros en santé. On constate un écart de maturité dans la lutte contre la fraude, mais un rattrapage rapide est constaté du fait d'un niveau de menace observé par tous. Cette menace se compose de plusieurs pans : le 100 % santé, qui a ouvert un nouveau marché de la fraude avec le panier de soins (Optique, Dentaire, Audioprothèse), en plus de fraudes déjà existantes sur l'hospitalisation, le transport ou les soins infirmiers. Aujourd'hui, on constate un pic de fraude qui bouleverse les équilibres et fait réagir les entreprises du secteur. Un deuxième pan est venu accentuer le développement de la fraude : la libéralisation des centres de santé, qui a ôté les contrôles préalables des Agences Régionales de Santé pour l'ouverture de centres de santé. L'idée initiale, développée par deux ministres successifs de la santé, était de libéraliser les centres de santé pour lutter contre les déserts médicaux.

Ce qui a été constaté, c'est une dérive à grande échelle de certains acteurs qui font les choux-gras des journaux, en optique, en dentaire, en audioprothèse…

Il y a une quinzaine d'années, il suffisait d'appeler directement un ophtalmologiste pour prendre rendez-vous. Le patient se rendait alors au centre de santé et rencontrait l'assistante puis le praticien. Aujourd'hui, le parcours est davantage structuré : les rendez-vous se prennent sur des plateformes en ligne et le patient suit un protocole complet. L'assistante réceptionne la carte Vitale et, le cas échéant, la carte de mutuelle, avant que le patient ne soit automatiquement orienté vers des tests de vue et un examen du fond de l'œil, puis vers la consultation avec l'ophtalmologiste. Le parcours est similaire dans le domaine dentaire, où une radiographie préalable est systématiquement réalisée.

La qualité des intervenants n'est pas toujours facilement identifiable, et il est rarement vérifié si ces examens ont été effectués récemment. Avant de quitter le centre de santé, le patient récupère ses documents et règle un éventuel reste à charge.

Le 100 % santé a été exploité dans une logique financière avec une recherche de profit maximum. Rapidement la fraude est arrivée sous forme d'actes fictifs ou d'intervention réalisées par des professionnels non qualifiés pour effectuer certains actes.

Ce que vous évoquez, est-ce plus de l'abus que de la fraude ?

Quand il s'agit d'un acte médical fictif, il s'agit de fraude. Quand certains praticiens facturent en fonction du plafond des garanties, c'est également de la fraude. Un abus répété est par définition une fraude. Le vocabulaire en santé est très riche, permettant de justifier des pratiques qui ne le sont pas. En 2023, 72 % des cas de fraude identifiés concernaient des documents falsifiés, incluant de fausses factures ou des fausses déclarations.

Depuis sa création, le système de Sécurité sociale repose sur une confiance envers les professionnels de santé. Cependant, la société et les comportements ont évolué. Aujourd'hui, celui qui facture est également le bénéficiaire du paiement. De plus, avec la codification des actes facturés, il est très difficile de déterminer si l'acte médical est justifié ou même de savoir s'il a été effectivement réalisé. Le système manque désormais de lisibilité, ce qui complique considérablement la détection des abus et des fraudes. Les enjeux financiers restent considérables, se chiffrant à plusieurs milliards d'Euros.

Est-ce que les typologies de fraude ont évolué ? Vous évoquiez les professionnels de santé. On a le sentiment, peut-être à tort, qu'il y a des «bandes organisées» qui utilisent des outils technologiques, via les réseaux sociaux, et organisent la fraude à l'assurance santé avec parfois la «complicité» de l'assuré qui fournit sa carte vitale ?

Les professionnels de santé représentent aujourd'hui 70 % de la fraude en montant. Vient ensuite la fraude des assurés, dans un contexte économique contraint. En pratique certaines propositions circulent sur les réseaux sociaux pour réaliser une fraude à la mutuelle d'assurance avec un partage 50/50 sur les revenus générés par la falsification. Le fraudeur qui a initié la démarche se charge de l'ensemble du processus et l'assuré lui reverse ensuite sa part selon des modalités précises. Ce type de pratique n'existait pas avant le COVID.

Il existe également des faux documents. Il est parfois très simple de faire des montages pour créer une fausse facture, émanant d'un ostéopathe par exemple. Cette capacité de fraude est augmentée par l'intelligence artificielle, qui démultiplie les possibilités de fabrication et altération. C'est pour cette raison que les assureurs investissent et développent des outils pour contrer cette menace.

Est-ce que l'optimisation de la télétransmission et la mutualisation, des datas liées à un acte de santé, ne seraient pas des éléments qui favoriseraient la lutte anti-fraude ?

Un de nos enjeux majeur concerne la réconciliation des pistes d'audit. Aujourd'hui pour les remboursements en santé, une partie est prise en charge par la caisse primaire, l'autre par la mutuelle d'assurance, qui recourt souvent à un

« tiers payeur ». Il n'existe pas de centralisation permettant une vue unique et globale des détails et des paiements. Il y a un vrai sujet de réconciliation des pistes d'audit pour enregistrer des décaissements de prestations de manière plus fiable. Il est essentiel que les acteurs du secteur comprennent précisément ce qu'ils payent, grâce à des points de contrôle basées sur des données de prestations complètes et un historique détaillé.

Concernant la mutualisation des données, elle permettrait bien sûr de lutter contre la fraude.

Est-ce que cette mutualisation des données de remboursement de prestations peut se faire réellement ? Est-ce que tout le monde a la volonté de le faire ?

D'un point de vue très macroscopique, oui, il faudrait mutualiser. Mais la mutualisation nécessite le consentement de tous les acteurs, y compris l'Assurance maladie. Avant cela, un travail préparatoire doit être mené afin de définir ce qui a réellement un sens à mutualiser. Un projet de loi relatif à la fraude sociale et fiscale est actuellement en discussion, ce qui ouvre de nouvelles perspectives.

Concernant l'écosystème des acteurs du secteur de l'assurance et de la prévoyance, il faut être pragmatique : partager l'intégralité des données relatives aux remboursements, par exemple dans une base de données géante, n'est pas « La » solution.

Aujourd'hui, grâce à la technologie, il est possible d'échanger des données de manière sécurisée via des protocoles de chiffrement, permettant de traiter, de calculer et d'interpréter l'information sans avoir à la déchiffrer.

La mutualisation des données peut susciter des inquiétudes, alors qu'elle est nécessaire face à des fraudeurs qui n'ont aucune obligation réglementaire et qui opèrent parfois en dehors du territoire national. Les acteurs légaux ont, eux, des contraintes réglementaires et travaillent en silos. Il est donc indispensable de se poser la question de la manière dont un dispositif performant peut être mis en place dans ce contexte contraint.

Des améliorations sont possibles par rapport à ce que nous proposons aujourd'hui, mais cela suppose des avancées législatives et une volonté de la part des acteurs du secteur.

Certains acteurs parlent de la nécessité d'avoir un tiers de confiance ?

L'histoire et l'organisation de l'ALFA reposent sur la nécessité même de construire des socles communs pour échanger : un cadre avec des règles et des outils. Il y a seulement quelques organismes comme l'ALFA dans le monde. Il faut maintenant une réponse collective au problème d'abus et de fraude qui touche tous les acteurs. Chaque organisme d'assurance doit agir sur son portefeuille, mais

l'évolution de la fraude vers un phénomène de plus en plus professionnel nécessite de trouver des réponses collectives. La mutualisation permettrait d'aller plus loin et d'identifier plus rapidement les menaces. Pour répondre directement à votre question, l'idée d'un tiers de confiance n'est pas saugrenue : une organisation spécialisée dans la lutte contre la fraude pourrait accompagner et soutenir l'ensemble des acteurs du secteur.

Cela pourrait être le rôle de l'ALFA ?

Oui, mais c'est à nos membres qu'il appartient de se positionner. Nous travaillons sur des propositions qui font sens au regard de ce qui a été construit depuis notre création il y a 36 ans. Soutenus par le financement de nos adhérents, nous avons un rôle à jouer, d'autant que l'urgence sur ce sujet complexe se confirme, réunissant les intérêts communs de multiples acteurs.

N'y a-t-il pas aussi nécessité d'une articulation public/privé sur le sujet de la fraude ?

Il n'y a pas, aujourd'hui, de discussion opérationnelle entre le régime obligatoire et les organismes complémentaires en santé, tout simplement parce que ce n'est pas prévu dans les textes. Nous sommes favorables à la proposition de loi du député Cyrille Isaac Sibille (NDLR : voir son ITW dans ce document) visant à améliorer la coordination entre l'assurance maladie obligatoire et les complémentaires santé dans la lutte contre la fraude, qui devrait être examiné prochainement. Il est indispensable de travailler ensemble et de faire émerger cette complémentarité.

Est-ce que nous sommes qu'au début d'un « tsunami » de fraudes générées par l'IA, même si celle-ci permet d'intercepter un très grand nombre de fraudes ?

Je ne crois pas à un tsunami de fraude générées par l'IA aujourd'hui. La fraude est simplement devenue un peu plus facile qu'avant à réaliser. Ce qui m'inquiète plus, en termes de sécurité, est le changement de paradigme imminent lié à l'informatique quantique dans les cinq prochaines années. Tous les fondamentaux de sécurité que l'on connaît, seront à revoir. Pour revenir à l'IA, s'il y a un an nous avions des assistants GPT, aujourd'hui nous voyons apparaître des agents capables d'exécuter des actions pour nous, comme l'achat d'un billet d'avion ou la réservation d'un hôtel. Ces agents seront intégrés dans nos navigateurs Internet du grand public très prochainement. Les ruptures technologiques vont impacter nos modèles actuels. Nous sommes dans un monde qui bouge à une vitesse sans précédent. Le problème n'est pas technique ou technologique, mais concerne la priorisation et l'adaptation des humains à ces nouvelles technologies. Il est donc nécessaire de prendre des mesures raisonnables et pragmatiques pour progresser, sans attendre la « solution parfaite » qui n'existera jamais.

Le secteur de l'assurance a d'immenses vertus. Il a parfois quelques défauts, son temps de réaction à certains sujets ?

Oui, l'assurance est une industrie du temps long, mais aujourd'hui le secteur de l'assurance « a plus mal » qu'avant. La fraude s'amplifie avec des montants assez colossaux, le contexte économique reste complexe, les risques climatiques augmentent, et la situation géopolitique est instable, le tout dans un monde qui change très vite. Nous ne sommes plus dans les mêmes temporalités sociétales qu'il y a quelques décennies. Le temps de l'action est venu.

[1]Pour conclure, pouvez-vous nous résumer la mission d'ALFA ?

L'Agence de lutte contre la fraude à l'assurance (ALFA), est un organisme professionnel créé en 1989 à l'initiative des sociétés et mutuelles d'assurances. Constituée en association à but non lucratif, elle a pour mission de promouvoir la lutte contre la fraude à l'assurance sous toutes ses formes et d'établir une interface entre le secteur de l'assurance et les pouvoirs publics.
Pendant longtemps cantonnée aux assurances de biens et responsabilité, l'association s'est ouverte progressivement à toutes les branches d'activité. Forte de plus de trente-six années d'existence et de dix collaborateurs engagés, l'agence regroupe aujourd'hui plus de 345 organismes d'assurance, incluant des entreprises d'assurances, des mutuelles et des institutions de prévoyance. Près de 2 000 correspondants anti-fraude figurent dans les annuaires que tient à jour l'ALFA. Cette large représentativité permet à l'association de jouer un rôle central dans la coordination des efforts de lutte contre la fraude. L'ALFA, avec un conseil d'administration élargi en 2025, œuvre à la mise en place d'un écosystème de lutte anti-fraude plus résilient et mieux préparé. C'est un hub de la lutte antifraude.

2-https://www.securite-sociale.fr/files/live/sites/SSFR/files/medias/DSS/2024/Chiffres-cles-DSS-2023-ed24.pdf

3 -L'Agence de lutte contre la fraude à l'assurance estime que l'enjeu financier de la fraude à l'assurance en santé-prévoyance représente au moins 5 % des prestations payées dans ces branches,
soit 2,74 milliards d'Euros par an pour le seul secteur privé. La charges des prestations en 2023 est de 36,6 milliards d'Euros en santé et de 18,2 milliards d'Euros en prévoyance, selon France Assureurs

4- https://www.ordre-chirurgiens-dentistes.fr/actualites/dix-ans-de-procedures-intentees-par-lordre-contre-les-centres-deviants/

2 . L'IA, NOUVEL ATOUT DES ASSUREURS CONTRE LA FRAUDE SANTÉ ?

Face à la montée des fraudes à l'assurance santé, les méthodes de contrôle traditionnelles atteignent leurs limites. Les volumes de données à traiter explosent, les parcours de soins sont de plus en plus dématérialisés, et les schémas frauduleux gagnent en sophistication : faux arrêts de travail, documents contrefaits, exploitation massive du SNDS. Dans ce contexte, l'intelligence artificielle (IA) s'affirme comme un levier stratégique indispensable.

Nouveaux résultats illustrant la puissance de l'approche automatisée

En 2024, les **fraudes aux arrêts de travail** ont représenté **42 M€**, dont près de **60 % ont pu être bloqués avant versement**, démontrant la pertinence d'un ciblage algorithmique combiné à des contrôles renforcés (Ameli). De même, le secteur des **audioprothèses** s'est révélé particulièrement vulnérable : **115 M€ de fraudes** y ont été détectés et stoppés en 2024, soit une multiplication par cinq en un an, grâce au déploiement de dispositifs numériques de contrôle et d'alertes renforcées (Ameli).

Pourquoi privilégier l'IA dans la lutte antifraude ?

- Efficacité préventive : l'IA permet de bloquer les fraudes avant qu'elles ne génèrent un préjudice financier.
- Ciblage plus fin : ces outils identifient les anomalies les plus subtiles (ratios inhabituels, comportements hors normes) et affinent la mise sous surveillance des dossiers sensibles.
- Allègement des processus humains : les équipes se concentrent sur la qualification des cas complexes, tandis que l'IA filtre les masses de données, rendant les contrôles plus rentables et mieux ciblés.

Outils actuels de l'IA en santé

Les solutions aujourd'hui déployées reposent principalement sur trois piliers :

Le scoring prédictif

Chaque dossier de remboursement est évalué par un système d'IA qui lui attribue un score de risque basé sur des données historiques : profil patient, professionnel, codes d'actes, volumes pratiqués. Ce mécanisme permet de prioriser les dossiers suspects pour enquête.
Des acteurs comme Shift Technology collaborent déjà avec la CNAM et plusieurs complémentaires santé pour affiner ces modèles.

La détection de motifs anormaux

Les algorithmes repèrent des irrégularités statistiques imperceptibles à l'œil humain : prescriptions répétitives, volumes inhabituels d'actes, incohérences codées. L'analyse peut être spatiale (clusters géographiques d'anomalies) ou temporelle (pics soudains d'activité).

L'analyse comportementale

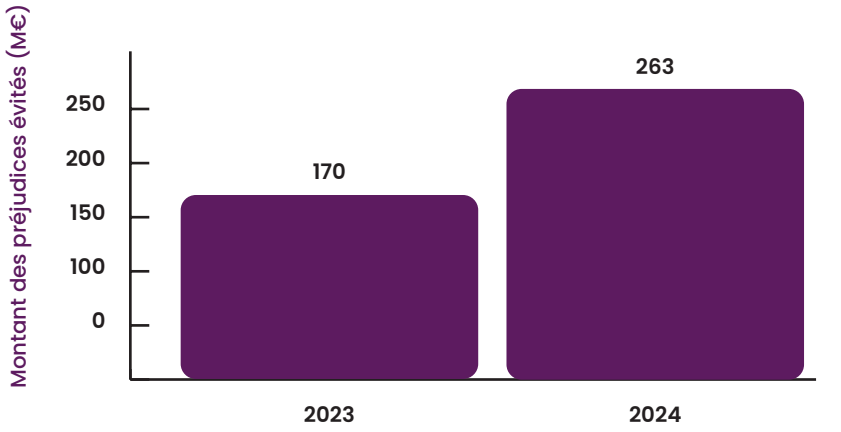
Enfin, l'analyse comportementale a pris une place centrale : les plateformes comparent les pratiques d'un professionnel ou d'un assuré à celles d'un groupe de référence. Lorsqu'un prestataire affiche des facturations disproportionnées par rapport à ses pairs, un signal est automatiquement activé. Cette orientation comparative permet ainsi d'identifier les écarts les plus significatifs, combinant efficacité et rapidité dans le ciblage des contrôles (Ameli).

Gains observés

L'usage de l'IA a déjà permis des résultats concrets :

- Rapidité : les outils automatisés traitent des millions de lignes en quelques secondes, permettant de bloquer des remboursements suspects avant paiement. Shift Technology évoque des gains importants de productivité « Grâce à notre solution, il est certain que les équipes de contrôle et de gestion anti-fraude gagnent énormément en productivité. D'une part car il est parfois difficile, voire impossible de détecter certaines suspicions, et d'autre part, le fait de pouvoir centraliser la gestion des cas dans un seul et même outil et un gain de temps important pour maximiser la performance opérationnelle ».
- Précision : l'IA excelle dans la détection de signaux faibles. En 2024, une part importante des fraudes liées aux arrêts maladie a pu être stoppée avant versement grâce à la combinaison entre IA et contrôles ciblés.
- Efficacité économique : près de 263 M€ de préjudices ont été évités avant remboursement en 2024, soit une hausse de +55 % en un an (Ameli).
- Optimisation des ressources : les équipes humaines se concentrent sur la qualification des cas complexes, laissant à l'IA le soin de filtrer les masses de données.

Fraudes stoppées avant remboursement grâce à l'IA (2023-2024)



Source : EN3S / Ameli

Concernant les 263 M€ de préjudices, **Shift Technology** précise « *Nous le constatons chaque jour : la détection de fraude avant paiement est la pierre angulaire d'un dispositif anti-fraude performant. Bien que la détection après paiement produise également des résultats importants, via une approche agrégée par professionnel de santé générant dissuasion et recouvrement, la détection et le blocage avant paiement présentent de nombreux avantages : un processus d'investigation allégé, l'absence de procédures de recouvrement souvent chronophages et coûteuses. En détectant la fraude en amont, les assureurs gagnent en productivité et en efficacité dans leur lutte contre la fraude. Chez Shift, nous proposons ainsi un processus de détection avant paiement (en temps réel pour les PEC et sur les factures) pour répondre à ce besoin.* »

Perspectives et défis

La montée des faux documents générés par IA – certificats médicaux, ordonnances, sinistres fictifs – illustre l'importance de ces outils. Ces falsifications deviennent quasiment indétectables sans recours à des technologies avancées. Malgré ses promesses, l'IA n'est pas exempte de limites :

- Les **faux positifs** persistent, nécessitant une supervision humaine systématique pour éviter les erreurs d'appréciation.
- Le cadre légal se renforce : **l'IA Act**, entré en vigueur en 2024, impose des exigences strictes en matière de transparence, d'explicabilité et de contrôle humain.
- La protection des données de santé demeure un impératif, avec des contraintes renforcées en matière d'anonymisation, de traçabilité et d'auditabilité.

CHIFFRES CLÉS À RETENIR

- **42 M€ de fraudes aux arrêts de travail en 2024**, dont près de 60 % stoppés avant versement
- **115 M€ de fraudes détectées dans les audioprothèses en 2024**, soit ×5 en un an
- **263 M€ de préjudices évités** avant remboursement grâce à l'IA en 2024 (+55 % en un an)
- **60 % des fraudes liées aux arrêts maladie** stoppées avant versement en 2024
- L'IA Act (2024) classe les systèmes d'IA en santé comme **applications « à haut risque »**, imposant transparence et supervision humaine

David Dumas-Lattaque
est Head of Customer Success France - Health & Life de SHIFT TECHNOLOGY. Son interview a été réalisée le 19/09/2025.

Pouvez-vous nous parler des enjeux et de l'évolution de la fraude en santé ?

La fraude en santé va certainement continuer d'évoluer vers plus d'industrialisation et de sophistication : réseaux organisés, inventions de prestations, facturation d'équipements fictifs ou gonflement des montants, utilisations de faux documents créés par une IA… La digitalisation accroît à la fois les opportunités de fraude et surtout les capacités de détection. Face à cela, une lutte efficace exige une détection en temps réel, une analyse multi-sources (données assureurs, CPAM, bases de données externes) et multi-format (données structurées et documents) ainsi que des processus automatisés pour prioriser les investigations. Un renforcement des échanges inter-acteurs, encadrés juridiquement, permettra d'accélérer ce travail et investir dans des modèles adaptatifs et évolutifs. La mise à disposition de données de qualité et la collaboration sectorielle seront clés pour contenir l'impact financier lié à ce fléau.

Comment évoluent les typologies de fraudes observées dans le champ de l'assurance santé aujourd'hui ?

Les typologies de fraude en assurance santé évoluent et se diversifient. On observe aujourd'hui deux grandes tendances :

- **Fraude des professionnels de santé :** elle représente une part importante des montants détectés (souvent plus de 70% voire 80% selon les bilans), du fait d'opérations plus rentables et organisées (actes fictifs, surfacturation de dispositifs, facturation de prestations non réalisées, collusion avec des assurés). Ces fraudes tendent à être « industrialisées » avec des réseaux structurés, des schémas complexes des fraudeurs qui se spécialisent. Nous voyons régulièrement l'exemple avec des collusions entre professionnels de Santé, opticiens et audioprothésistes, ou des PS prescripteurs. Certaines fraudes représentent des enjeux financiers de plusieurs dizaines voire centaines de milliers d'Euros (par exemple des trafics de médicaments)

■ **Fraude des assurés :** nous observons toujours des volumes significatifs et croissants (déclarations mensongères, actes non réalisés, faux documents via des recours à des procédés numériques plus élaborés) parfois plus visibles grâce à l'intensification des contrôles et au développement de nouveaux algorithmes de détection. Nous constatons également une industrialisation de cette typologie de fraude via les réseaux sociaux. Les montants unitaires sont en général plus faibles que pour la fraude des praticiens, mais le nombre d'actes frauduleux reste important.

Les cas de fautes tels que les doubles paiements, ou encore les erreurs de facturations telles que les exonérations, sont toujours observés.

Que peut-on dire des coûts liés à la Fraude pour les assureurs ?

Selon plusieurs sources, nous pouvons considérer qu'en moyenne les pourcentages de fraude et paiements à tort en assurance santé représentent entre 5 et 10% du montant des prestations versées.
Avec nos solutions, nous observons des résultats de gains pouvant aller jusqu'à 10€ par personnes protégées par an, soit par blocage de paiement soit par récupération de sommes indues. Les montants détectés peuvent quant à eux représenter facilement le double voire le triple des montants économisés selon les contextes.

Comment l'Intelligence Artificielle est-elle concrètement utilisée pour détecter et traiter la fraude ?

Nos solutions exploitent plusieurs briques d'IA complémentaires pour lutter contre la fraude, les abus et les paiements à tort :

■ Préparation et enrichissement des données : nettoyage, normalisation et reconstitution d'entités (corrections orthographiques, rapprochement et consolidation d'identifiants), afin d'obtenir des jeux de données fiables et exploitables.

■ Traitement du langage naturel (NLP) et grands modèles de langage : extraction d'informations à partir de textes libres (courriers, rapports, échanges), catégorisation automatique et génération d'observations sur des contenus non structurés.

■ Apprentissage automatique (ML) : modèles supervisés pour prédire la probabilité de fraude et prioriser les alertes au sein de scénarios métiers ; modèles non supervisés pour détecter des tendances émergentes et des anomalies inédites.

■ Analyse documentaire et visuelle : lecture automatique de documents (OCR), extraction de métadonnées, comparaison d'images et détection de falsifications ou de duplications.

■ Analyse de graphes et des réseaux : mise en lumière des relations entre acteurs (assurés, professionnels, prestataires) pour identifier des schémas organisés et des réseaux de fraude.

Ces composants sont orchestrés ensemble : la qualité des données alimente les modèles, le NLP et l'analyse documentaire enrichissent les signaux, et l'analyse de réseau permet de détecter les schémas structurels. Le résultat est un dispositif capable de détecter plus tôt, classer et prioriser les cas à investiguer, et orienter les actions correctives pour faciliter le travail aux gestionnaires.

Peut-on parler d'aide à la décision ou est-on déjà sur de l'automatisation ?

Les solutions existantes sont des outils d'aide à la décision qui automatisent un grand nombre de tâches et de calculs que les gestionnaires mettraient parfois des heures voire des jours à réaliser. Néanmoins, il n'est pas possible aujourd'hui d'automatiser le traitement de bout en bout d'une alerte de fraude et de bloquer définitivement une prestation sans qu'il y ait eu de contrôle humain. La CNIL l'interdit. Le résultat de la détection et l'instruction de l'alerte générée par les algorithmes seront toujours validés par un gestionnaire.

Et concernant la transparence des algorithmes et la traçabilité des décisions ?

Chacun de nos clients a la connaissance des scénarios intégrés à la solution qu'ils exploitent. Ce sont eux qui définissent leur stratégie de lutte anti-fraude et Shift Technology alimente ensuite la base de scénarios en production en fonction de ceux qu'ils auront sélectionnés. Les scénarios varient en fonction du domaine de soins, du type de suspicion recherchée (fraude, abus, fautes etc.) et du type de fraudeur visé (assuré, professionnel de santé ou encore collusion) ; Chaque alerte générée par un ou plusieurs scénarios présente dans l'interface utilisateurs l'ensemble des variables explicatives calculées ayant mené à la suspicion, avec un score global de suspicion dédié. Les actions des gestionnaires sont également tracées dans la solution pour faciliter le suivi.

Comment évitez-vous les biais algorithmiques ?

Plutôt que d'aborder la fraude comme un problème unique et global, nous décomposons la problématique en sous-ensembles que nous contrôlons séparément. Cela nous permet de garder la maîtrise sur le comportement global de la solution.

Nous nous concentrons sur l'analyse de comportements suspects, et non sur de simples corrélations statistiques. Concrètement, des données comme le lieu de résidence, le nom de famille ou la nationalité ne sont jamais utilisées comme facteurs de suspicion. Elles ne peuvent servir que de repères techniques (par exemple pour mesurer des distances ou détecter des liens de parenté), mais jamais comme critères déterminants. Au-delà de l'éthique, cela éviterait sur-

tout de générer des alertes non pertinentes.

Enfin, notre IA n'a pas vocation à prendre de décision finale. Elle fournit un score de suspicion ainsi que les facteurs explicatifs qui ont conduit à cette alerte. C'est ensuite un gestionnaire ou un enquêteur qui analyse les résultats, mène l'investigation et décide de l'action à entreprendre. L'IA est donc un outil d'aide à la décision, qui permet de travailler plus vite et plus efficacement.

L'IA permet-elle aussi de prévenir la fraude en amont ?

Après avoir généré des alertes sur des assurés ou professionnels de santé, notre solution permet aux gestionnaires de réaliser des campagnes de contrôles sur les plus grands fraudeurs créant ainsi, pour la majorité d'entre eux, un effet dissuasif. Grâce à ces actions, nous constatons une diminution des volumes de fraude chez les personnes ciblées. Nous sommes capables de mesurer avec précision les impacts.

Au-delà de son effet dissuasif, notre solution s'intègre aux systèmes d'information des complémentaires santé afin de bloquer, avant paiement, toute prestation faisant l'objet d'une suspicion, qu'il s'agisse d'une fraude ou d'une faute, sur les flux tiers payant et hors tiers payant.

L'utilisation de l'IA contre la fraude par les acteurs de l'assurance santé est-elle une pratique courante ?

Oui, l'usage de l'IA pour la détection de fraude, abus et paiement à tort en assurance santé se généralise progressivement.
Les plus grands acteurs du marché ont investi dans des solutions comme celles de Shift Technology ou bien dans des équipes de Data scientists afin de développer des cas d'usage autour de cette thématique. Des modèles hybrides existent parfois. Les acteurs de taille intermédiaire et de plus petites mutuelles ont suivi la tendance.

Quels sont, selon vous, les freins majeurs à une meilleure mutualisation des données de prestations santé dans le secteur ?

Shift Technology a initié une base de détection mutualisée en assurance santé et prévoyance qui consiste à identifier des suspicions de fraude, abus et fautes à partir d'historiques de données pseudonymisées de bénéficiaires (assurés) issues de plusieurs organismes complémentaires. Seuls ceux ayant souhaité adhérer à cette initiative ont accès à cette base. Cette mise en commun d'informations permet ainsi d'appliquer des scénarios spécifiques et générer des alertes qui n'auraient pu être créées sans ce croisement de données. L'objectif est double : étendre la détection avec de nouveaux scénarios spécifiques afin d'identifier davantage de cas et réaliser des économies additionnelles (estimation de +5% à 10%).

Les principaux freins sont souvent d'ordre réglementaire. À titre d'exemple, la CNIL a récemment restreint l'exploitation de certaines données à des fins de lutte anti-fraude. Cela a malheureusement réduit l'efficacité de certains types de détection pour lesquels ces informations étaient nécessaires afin de lever des suspicions.

Existe-t-il des ponts de collaboration avec les complémentaires santé et l'Assurance Maladie, sur la gestion coordonnée de la fraude ?

Ce qui existe déjà dans le secteur de l'assurance santé :

- Des partages d'informations encadrés : échange de données ciblées entre OCAM (parfois via des conventions ou via des intermédiaires sécurisés) pour des cas de suspicion confirmée.
- Des instances bilatérales ou multilatérales : groupes de travail sectoriels, observatoires de la fraude ou partenariats avec des gestionnaires mutualisés (ex. certaines structures inter-assureurs).
- Des initiatives associatives : organisations comme l'ALFA via la mise en place des circulaires, API ou règles de gouvernance pour faciliter les échanges entre membres.

Les OCAM sont assez promoteurs de l'idée du développement d'une meilleure collaboration avec l'Assurance Maladie. Ce sujet a notamment été introduit dans le PLFSS 2025 avec par exemple le fait qu'en cas de soupçon de fraude l'Assurance maladie et les organismes complémentaires pourront échanger des informations ciblées sur l'auteur présumé ainsi que sur les actes et prestations concernés.

Les professionnels de santé expriment des craintes, non ?

Nous n'élaborons pas nos modèles sous forme de boîtes noires visant à résoudre un problème de bout en bout. Nous décomposons la problématique (par ex. la détection de fraude) en sous-problèmes distincts, que nous traitons séparément, ce qui nous permet de conserver une maîtrise fine du comportement global du système. Par ailleurs, nos algorithmes cherchent à repérer des comportements suspects (schémas, enchaînements d'actions, connexions entre acteurs) plutôt qu'à s'appuyer sur de simples corrélations statistiques. Ainsi, nos analyses restent objectives et factuelles, limitant tous risques de biais dans la détection. Seuls les professionnels de santé présentant des motifs sérieux de suspicion sont soumis à des contrôles ou au blocage de prestations.

La fraude santé peut-elle vraiment être réduite durablement, ou faut-il plutôt parler de « gestion du risque fraude » ?

Nous n'élaborons pas nos modèles sous forme de boîtes noires visant à

La fraude continuera très probablement d'évoluer, portée par l'inventivité des fraudeurs et l'émergence de nouveaux schémas. Il est difficile de prédire si le volume d'opérations suspectes augmentera fortement, mais une chose est certaine : entre les évolutions réglementaires et l'arrivée de nouvelles technologies, les dispositifs de détection doivent s'adapter en permanence. L'amélioration continue des modèles et l'intégration de nouveaux scénarios seront essentielles pour bloquer les prestations indûment versées et neutraliser les fraudeurs. Ces contrôles, qui peuvent aboutir à des sanctions de la part des complémentaires santé, contribuent également à renforcer l'effet dissuasif obtenu grâce à des solutions comme celle de Shift Technology.

Voyez-vous émerger de nouvelles menaces (deepfake de documents, IA générative, etc.) dans le domaine de la fraude ?

Des nouvelles typologies de fraude sont apparues en exploitant différents canaux tels que les réseaux sociaux. Par exemple, certains fraudeurs, usurpant l'identité de professionnels de santé, sont entrés en contact via Snapchat avec des assurés complices pour créer des facturations d'actes fictifs. Grâce à des échanges d'informations sur les garanties et les données liées au contrat des assurés, plusieurs dizaines de milliers d'Euros ont été rattachés à ces fraudes documentaires.

Autre exemple, les faux documents créés à partir d'intelligence artificielle générative seront bien plus difficiles à détecter par un humain, c'est la raison pour laquelle la poursuite de la recherche et développement sur des scénarios évolués analysant le contenu des documents ainsi que leur métadonnées sera clé pour continuer de lutter efficacement contre ces nouvelles pratiques frauduleuses.

Quelles innovations techniques ou réglementaires pourraient faire progresser la lutte contre la fraude dans les 3 à 5 ans ?

Plusieurs axes d'amélioration sont identifiés :

- La poursuite de la détection et le renforcement des analyses de réseaux grâce à de nouveaux algorithmes afin de révéler les cas de collusions les plus complexes.
- La généralisation du partage d'informations entre OCAM, comme l'initiative de Shift Technology évoquée précédemment, et entre les OCAM et le régime obligatoire tout en respectant la protection de données personnelles et encadrant juridiquement ces collaborations. L'idée est de pouvoir mieux partager les signaux de suspicion de façon sécurisée et traçable.
- L'exploitation d'agents intelligents (IA agentique) intégrés aux solutions afin d'accélérer les investigations et automatiser certaines étapes encore réalisées manuellement aujourd'hui. Par exemple, un contact de l'assuré ou PS, une analyse de pièces justificatives reçues après un contrôle, etc.

Comment Shift Technology analyse les cas et facilite les investigations et traitement ?

La solution de Shift Technology analyse de manière récurrente et, selon les contextes, en temps réel, les données transmises par les assureurs (tiers payant et hors tiers payant), et restitue les résultats sous forme d'alertes dans une interface dédiée. Cette interface, outil d'aide à la décision utilisé par des gestionnaires spécialisés, permet de comprendre l'analyse via le partage des variables explicatives associées aux cas suspects, et facilite l'investigation grâce à un ensemble de fonctionnalités intégrées (historique des actions réalisées par les gestionnaires, réception de pièces justificatives, intégration du processus de qualification des alertes étape par étape, etc.).

La centralisation des traitements dans un outil unique permet la gestion complète d'un dossier, de sa détection à sa clôture, avec calcul automatique des économies reconnues et présentées sous la forme d'un reporting intégré. La restitution de ces métriques nous permet d'assurer un pilotage de la performance avec nos clients en vue d'améliorer continuellement le dispositif. Par ailleurs, cette solution permet également de réaliser un certain nombre d'analyses et d'exploration à la main des gestionnaires grâce à une restitution claire et structurée des données.

3. QUAND LA MACHINE SUSPECTE… MAIS NE JUGE PAS ?

L'intelligence artificielle renforce la lutte contre la fraude santé, mais elle demeure avant tout une **vigie numérique**, pas un juge. En 2024, les algorithmes ont repéré des comportements atypiques, actes médicaux répétitifs, volumes d'actes déraisonnables ou incohérences statistiques, et orienté les contrôles vers les cas les plus sensibles. Toutefois, seule l'expertise humaine permet de qualifier ces alertes en fraude avérée.

La qualification humaine, indispensable

Aussi performants soient-ils, ces systèmes génèrent des faux positifs. Un professionnel ou un assuré peut être injustement signalé, par exemple lorsqu'un centre médical en zone rurale pratique des volumes élevés d'actes justifiés par une population vieillissante, ou lorsqu'une spécialisation régionale explique des prescriptions atypiques. Dans un cas cité par la CNAM, un pharmacien avait été signalé pour des prescriptions d'hypnotiques en excès ; l'analyse métier a démontré que sa région souffrait d'un taux particulièrement élevé de troubles du sommeil. Sans ce regard humain, il aurait pu être sanctionné à tort (EN3S).

Un modèle organisationnel hybride

Ce constat justifie pleinement le recours à un **modèle hybride** où l'IA détecte et oriente, tandis que les équipes humaines valident, approfondissent ou écartent les alertes. Ce mode de fonctionnement est recommandé dans les secteurs réglementés, y compris l'assurance santé, pour garantir équité et fiabilité, conformément aux exigences du **RGPD** selon lesquelles toute décision automatisée ayant des effets significatifs doit être vérifiée par un humain.
Des acteurs comme Shift Technology fournissent des outils explicables ("white box"), permettant de comprendre pourquoi un dossier a été signalé et de faciliter ainsi la gouvernance humaine.

Enjeux éthiques et réglementaires

Par ailleurs, l'adoption de ce modèle répond à une double exigence : éthique (garantir la justice et l'acceptabilité des process) et réglementaire. L'**IA Act**, entré en vigueur en 2024, impose pour les outils à risque élevé, tels que ceux appliqués à la santé, une **transparence**, une **auditabilité** et une **supervision humaine** obligatoire (Commission européenne). De même, la **Stratégie nationale IA en santé** souligne la nécessité de systèmes dignes de confiance, responsables et explicables, intégrant l'humain à chaque étape du cycle de décision (Ministère de la Santé 2025–2028).

En définitive, l'IA n'est pas un substitut, mais un outil de vigilance au service des experts. C'est cette alliance qui permet de préserver la confiance entre assureurs, soignants et assurés, tout en renforçant la robustesse du système de santé.

Yann Abeloos
est Directeur Général Adjoint
en charge du BPO – Gestion Déléguée – Tiers-Payant de CEGEDIM Assurances.
Son interview a été réalisée le 05/09/2025.

Comment évoluent les typologies de fraudes observées dans le champ de l'assurance santé aujourd'hui ?

Quelques nouveautés, sur ce sujet de la fraude, impactent essentiellement le secteur de l'assurance santé.

- D'un côté, des outils d'intelligence artificielle de génération de fausses factures et de l'autre des faux documents produits pour deux raisons essentielles. Pour générer des fausses demandes de remboursement de frais de santé qui n'ont pas lieu d'être : remboursement dentaire, kinésithérapie, ostéopathie, …
- Et de l'autre générer un faux document pour souscrire une assurance santé et ensuite demander des remboursements importants pour le même acte auprès de plusieurs acteurs.

Nous pouvons avoir la même chose côté professionnels de santé. Un professionnel de santé peut produire de faux documents pour être conventionné avec un opérateur de tiers payant et ensuite envoyer des fausses factures pour être remboursé. Nous pouvons aussi avoir des factures de faux kinésithérapeutes, opticiens, audiologues,… . Ces pratiques sont largement facilitées avec l'intelligence artificielle et ces générations de fausses factures deviennent un peu plus compliquées à identifier.

Un autre phénomène plutôt nouveau. Sur les réseaux sociaux, des personnes encouragent des gens à frauder. Les fraudeurs demandent une copie de la carte de tiers payant, s'occupent de faire des envois de fausses factures aux complémentaires santé et propose le partage à 50 % du remboursement. Le réseau social sert de mise en contact des acteurs de la fraude avec des assurés «lambda» pour générer une fraude à bénéfice partagé. Il s'agit d'une pratique de plus en plus fréquente, sur des réseaux connus.

En 2025, est-ce qu'il y a des tendances, des typologies de fraude plus importantes, en termes de volume de fraudes constatées ?

Les tendances dépendent des acteurs. Pour ce qui nous concerne, en tant qu'opérateur de tiers payant, comme nous avons davantage de délégation pour du tiers payant optique que pour du dentaire, naturellement, cela se retranscrit dans les tendances. Mais ce n'est pas pour autant qu'il y a plus de fraude d'un côté ou de l'autre. Nous constatons, en général, que la fraude est plutôt sur des actes à montants importants, donc assez naturellement, plutôt sur de l'optique et sur de l'hospitalisation, par exemple sur de la chambre particulière.

Est ce qu'il y a des zones grises sur la fraude détectée ? Il peut y avoir fraude intentionnelle ou erreur de bonne foi ?

Il y a les deux. C'est vrai, par exemple que ce que l'on détecte pour l'hôpital public, est davantage des erreurs. Des situations, par exemple, pour des patients en ALD (Affection Longue Durée) et pour lesquelles, des demandes de remboursements sont adressées à l'assurance santé complémentaire. Si cela relève plutôt de l'erreur, c'est néanmoins très important pour nos clients assureurs et pour leur compte technique. En revanche, lorsque des cliniques facturent des chambres particulières alors que l'assuré n'a pas séjourné dans les établissements, il s'agit là de tentatives de fraude.

Autre situation, des abus. Le cas classique de l'opticien qui connaît le niveau des garanties de l'assuré et qui va indiquer le montant maximum de la garantie : montures et verres. Tous ces scénarios génèrent des pertes techniques pour l'assureur, si la fraude n'est pas identifiée. Sur ce sujet, nous travaillons avec la même solution, celle de Shift Technology. Nous avons un partenariat exclusif pour un certain nombre de clients en assurance santé (14 à aujourd'hui). L'outil de Shift Technology permet de remonter des suspicions de fraude, ensuite nos équipes de gestion effectuent l'analyse et si la fraude est avérée, nous rejetons la facture ou réclamons le montant. Ensuite nous indiquons à nos clients, le volume de fraudes détectées, les remboursements fictifs évités, selon différents scénarios de détection.

La détection est permise grâce à l'apport de l'intelligence artificielle. Alors concrètement, comment est-elle utilisée ?

L'IA effectue l'analyse documentaire, dans le contenu des factures. Il y a plusieurs modules, par exemples comparer une facture avec des factures passées, ou sur un patient en ALD, l'IA va analyser la combinaison des médicaments facturés. Dans tous les cas l'outil remonte l'alerte, ensuite notre gestionnaire analyse et prend la décision finale. Lorsque l'argent à été récupéré suite à une fraude, cela octroie un scoring de pertinence de l'alerte initiale. Ce scoring favorise le côté apprentissage et les alertes pertinentes ainsi que l'utilisation de certains scénarios.

Que pouvez nous dire sur les scénarios que vous évoquez ?

Nous avons des dizaines de scénarios paramétrés. Par exemple des remboursements pour des séjours à l'hôpital qui dépassent 30 jours, des remboursements pour l'optique pour une demande d'équipement pour toute la famille, des lentilles pour des enfants de six mois… . Mais globalement, nous devons identifier des scénarios de fraude très impactants, pas très simples et avec des combinaisons de multiples facteurs. Nous nous concentrons sur les scénarios les plus pertinents, ceux qui génèrent des montants de fraude importants.

La détection de la fraude est automatisée et le traitement est-il toujours effectué par une intervention humaine ?

Exactement, le gestionnaire analyse et valide la pertinence de la détection par l'IA. Ensuite nous déclenchons la procédure s'il y a une fraude avérée pour récupérer le montant. Il n'y a jamais de demande de remboursement de la fraude totalement automatisés. Selon les scénarios, la pertinence de la détection de fraude effectuée par l'IA va être entre 30 et 50 %. Nos équipes de gestion de fraude sont importantes et nécessitent un niveau d'expertise dans l'assurance santé. Avec bien sûr, de la formation à nos processus, à l'enquête, à l'analyse. Dans certaines situations, nous pouvons faire appel à des médecins conseils qui peuvent dans certains cas nous donner leur avis sur une facture d'un dentiste, d'un opticien, … .

Revenons à votre partenariat avec Shift Technology ?

Nous proposons ensemble aux acteurs de l'assurance santé, la solution complète qui repose sur le logiciel de Shift Technology et la cellule de gestion de CEGEDIM Assurances. Cette offre est proposée à nos assureurs clients pour le tiers payant, à nos assureurs en gestion déléguée, et également dans le cadre de notre offre « logiciel ».

Quand une fraude est détectée et avérée, est-ce qu'il y a une traçabilité et une historisation de la fraude ?

Oui, c'est même le cœur de notre fonctionnement, c'est ce qui permet à chaque traitement d'analyser également les fraudes passées détectées, par exemple pour un même professionnel de santé. L'historique des fraudes démarre au lancement de notre partenariat avec Shift Technology, depuis 2021.

Est-ce que l'IA peut prévenir la fraude ?

Oui. Nous effectuons la détection de la fraude a posteriori, c'est à dire dès lors que la facture a été remboursée. Mais nous pouvons également bloquer le paiement de la prestation, par exemple au moment de la demande de prise en charge, pour l'hôpital, l'opticien, … . Après il y a des situations où ce n'est pas forcément facile, avec des gros volumes. Par exemple pour la pharmacie, nous traitons environ 4 millions de factures par semaine, et où nous devons tenir compte de la contrainte des délais de traitement liés à nos conventions avec ces professionnels de santé. Cela nous oblige à réaliser ces analyses de fraude dans un délai restreint. Le volume précédent est énorme par rapport aux 100 000 factures traitées pour l'optique. Nous devons donc nous concentrer sur les gros montants de remboursement.

Afin de réduire les tentatives de fraude en amont, est-ce qu'il y a aussi des actions de prévention, de communication, en amont de toute transmission de factures, pour sensibiliser les professionnels de santé ?

Ce que nous mesurons est l'effet dissuasif, qui n'arrive pas tout de suite. Mais pour les clients mis en production depuis un peu plus de deux ans, nous mesurons véritablement cet effet dissuasif de nos actions. Elles génèrent vraiment des gains pour les assureurs. Cet effet mesuré de la dissuasion se fait sur les mêmes professionnels de santé pour lesquels il y a déjà eu des détections d'erreurs, d'abus ou de fraude. Il y a quelques clients qui bénéficient de cette mesure, car celle-ci est liée à l'antériorité de la production que nous réalisons pour eux.

Nous allons parler des ponts de collaboration entre les assureurs santé et l'Assurance Maladie. Votre objectif est commun, la réduction de la fraude sur les prestations santé. Est-ce qu'il y a une forme de coopération publique/privé sur ces sujets de fraude ?

Aujourd'hui non. Et c'est malheureux. Il y a même une première question qui pourrait être. : « Est-ce qu'il y a un bon niveau de communication déjà entre l'Assurance Maladie et l'assurance complémentaire ? » La réponse est également non.

Bien sûr, il y a l'action de l'ALFA (Agence de Lutte contre la Fraude à l'Assurance) qui se concentre aujourd'hui sur la partie fraude avec la circularisation de situations de fraudes reproduites par des assurés. L'ALFA a très récemment décidé de s'ouvrir aux organismes tiers comme les opérateurs de tiers payant. Nous sommes devenus adhérents de l'ALFA depuis un mois. Nous devons travailler ensemble pour partager un peu plus largement sur le marché les pratiques frauduleuses qui se répètent chez les professionnels de santé.

Par ailleurs, j'ai lu récemment que l'Assurance Maladie voulait collaborer davantage avec les assureurs santé sur les sujets de fraude. Cela est extrêmement positif. Ensuite, il peut subsister des freins concernant une meilleure mutualisation des données. La donnée est une matière extrêmement précieuse pour chacun des assureurs qui proposent des produits de santé, des produits de prévoyance, … et la réglementation sur la protection des données (RGPD), fait que les acteurs sont très contrôlés. Par ailleurs, les acteurs du secteur voient la détection de fraude comme un avantage concurrentiel en réduisant les pertes techniques et en améliorant le résultat technique.

Un des points qui pourrait être intéressant de mutualiser entre acteurs du secteur est la situation des fraudeurs qui contractualisent des contrats santé chez plusieurs assureurs en même temps et qui se font rembourser plusieurs fois les mêmes soins. Cette détection est aujourd'hui impossible si nous n'avons pas d'analyse combinée des portefeuilles.

Vous êtes favorable à cette dynamique de collaboration, de co-construction entre acteurs pour rendre encore plus efficace la détection de fraude ?

Nous sommes complètement favorables pour faire progresser la lutte contre la fraude, tout le monde y gagnerait.

Il y a-t-il d'autres évolutions, innovations possibles sur ce sujet de la fraude en assurance santé ?

Concernant les professionnels de santé, quand la fraude est constatée, plutôt que de demander la restitution de la somme des prestations indues, ce qui n'est pas toujours simple, nous avons commencé à déployer des mécanismes de compensation sur les prochaines factures à recevoir. Si la réglementation nous aidait sur ce sujet, nous pourrions le faire davantage.

Les organisations représentatives des corporations de professionnels de santé que vous avez évoquées, n'ont-elles pas un rôle majeur pour sensibiliser à la nécessité de réduire la fraude ?

Elles ont un rôle à jouer. Mais pour l'instant, elles relayent plus les remontées de leurs adhérents qui trouvent anormal d'avoir à justifier leurs factures ou d'envoyer les ordonnances associées. Elles ont avant tout une posture de défense des intérêts de leurs adhérents.

Nous avons évoqué l'IA qui détecte la fraude. Parlons désormais de l'IA qui génère de la fraude documentaire.

L'assurance santé est un secteur très «processé» et nécessite également une demande de pièces assez importante. Avant de procéder au remboursement,

nous demandons la carte de tiers payant, le RIB, l'ordonnance, ... et cela met déjà un certain nombre de freins à la fraude. De plus, nous avons des développeurs qui travaillent pour permettre de détecter de faux documents générés par l'IA. Les nouvelles technologies permettent de détecter ces documents beaucoup plus facilement.

La fraude peut-elle être réduite durablement ?

La gestion de la fraude est un peu comme le risque cyber. Cela nécessite un travail continu avec les nouvelles technologies d'intelligence artificielle, mais aussi nos équipes de détection de fraude. Ces équipes ne cessent d'ailleurs de s'agrandir à mesure que le risque fraude s'amplifie. Quand un nouveau client entre en production, au départ, nous récupérons un historique de factures qui permet un gain immédiat. Ensuite, dans une logique de gestion courante de la fraude, passé deux ans, nous mesurons les effets dissuasifs. Nous constatons donc bien une baisse de la fraude.

Pour conclure ?

CEGEDIM Assurances joue clairement un rôle pour que le secteur de l'assurance santé constate moins de fraudes. Nous sommes l'entreprise avec le plus gros référentiel de professionnels de santé et d'assurés, nous sommes l'acteur leader du tiers payant, leader sur la partie logicielle et sur la gestion déléguée aujourd'hui. Nous permettons donc à nos clients, de se doter des outils et des moyens qui permettent d'avoir une gestion santé «propre». Nous devons rester à la pointe des outils proposés et sécuriser nos clients assureurs pour une gestion santé sans fraudeurs. C'est notre promesse. Tout le monde sait qu'il y aura de la fraude, mais en tout cas, nous arrivons à réduire les cas et les montants de fraude. Selon nos clients, nous leur générons entre 3 € et 7 € de gains par personne protégée. C'est extrêmement significatif dans un contexte marché où il y a de moins en moins de marge et une exigence de réduction des frais de gestion.

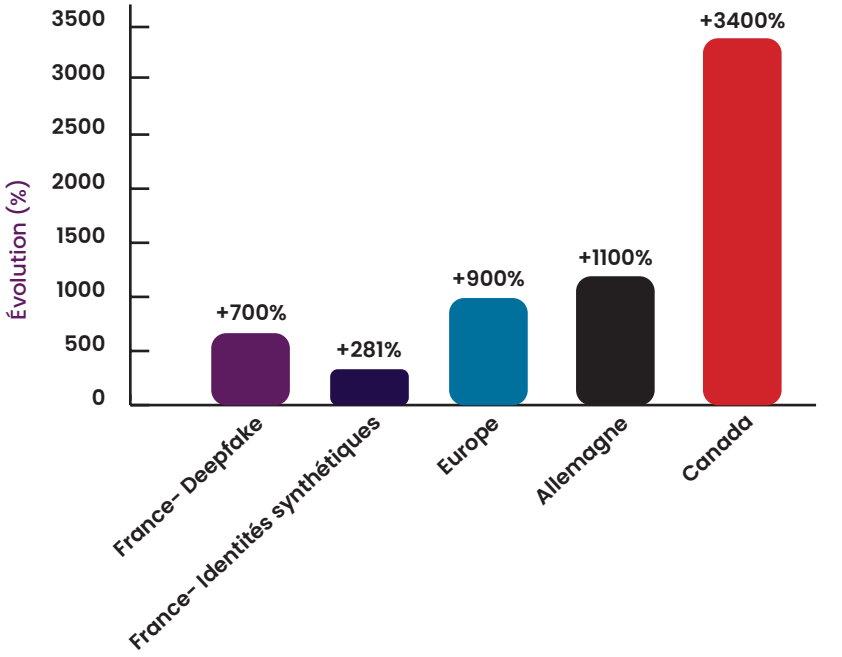
4. L'EFFET BOOMERANG : L'IA AU SERVICE DES FRAUDEURS

Alors que l'intelligence artificielle s'impose comme un levier stratégique pour lutter contre la fraude santé, elle révèle également une face sombre : celle d'un outil désormais exploité par les fraudeurs eux-mêmes. Entre 2023 et 2025, les cas de fraude via deepfakes médicaux, ordonnances générées automatiquement ou chatbots de phishing se sont multipliés, au point que la CNAM et la CNIL alertent désormais sur une industrialisation inquiétante de ces pratiques. Le paradoxe est clair : la technologie censée protéger les assureurs devient aussi une arme redoutable pour les attaquer.

Deepfakes et faux documents médicaux

Les fraudeurs disposent aujourd'hui d'outils accessibles pour générer certificats, ordonnances ou justificatifs de soins entièrement artificiels. Selon ShareID, les tentatives de fraude par deepfake ont augmenté de +700 % en un an en France, et l'usage de documents d'identité synthétiques a progressé de **281 %** (ShareID).

Explosion des fraudes IA (deepfakes et identités synthétiques) 2024-2025



Source : ShareID

En 2024, l'Assurance Maladie a stoppé plus de **13 M€ de fraudes liées aux fausses ordonnances**, grâce notamment au dispositif ASAFO-Pharma, qui a recensé plus de 7 300 suspicions, dont près de 75 % confirmées (Ameli). Ces pratiques sont facilitées par des kits vendus sur le dark web, permettant de produire des documents falsifiés d'un réalisme saisissant.

Le dark web, bien qu'il ne représente qu'une part minoritaire de l'internet global, enregistre **plus de 2,5 Millions de visites par jour** en 2023, avec une légère progression vers 2,7 Millions au printemps 2023 (Moneyzine via Tor). Un réseau dense de **places de marché illicites**, où l'on trouve données bancaires volées, faux documents et outils de fraude, est activement exploité par les cybercriminels. En France, ces places de marché jouent un rôle central dans le développement et la distribution de kits automatisés dédiés à la falsification médicale.

Phishing et usurpation via chatbots IA

Une nouvelle génération de campagnes de phishing exploite des chatbots dopés à l'IA. Ces faux assistants imitent les plateformes officielles (CNAM, mutuelles, centres de santé) et parviennent à convaincre les utilisateurs de divulguer leurs données personnelles. Selon Netskope, **8,4 utilisateurs sur 1 000 cliquaient chaque mois sur un lien de phishing en 2025**, contre seulement 2,9 en 2023, illustrant la progression fulgurante de ces attaques (Cofense).

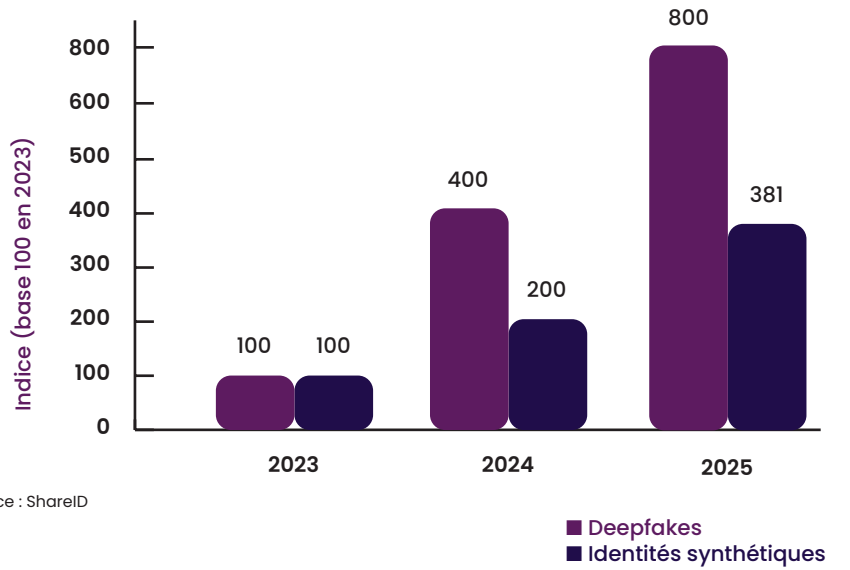
La CNIL et l'ANSSI confirment la hausse significative des signalements liés à ces faux chatbots, qui exploitent des conversations personnalisées pour paraître crédibles (CNIL).

Une fraude désormais industrialisée

Loin des fraudes artisanales d'autrefois, certaines formes de fraude se structurent désormais autour de réseaux. Un exemple concret : en 2023, la CNAM a mobilisé une task force nationale sur **sept centres de santé** suspectés de pratiques frauduleuses coordonnées. Ces investigations ont mené à des **déconventionnements et à des plaintes pénales** pour incohérences de facturation, soulignant l'existence de schémas frauduleux organisés au sein même de réseaux professionnels (Ameli).

Ces pratiques industrielles se doublent désormais d'innovations technologiques : les fraudeurs utilisent l'IA pour générer des bases de patients fictifs ou usurpés, et recourent à des kits automatiques diffusés sur le darknet pour produire en masse des ordonnances et dossiers médicaux falsifiés (CNIL). Ces méthodes s'accompagnent d'un enjeu financier considérable, avec des **préjudices potentiellement évalués en centaines de M€ par an**.

Explosion des fraudes par deepfakes et identités synthétiques (2023-2025)



Source : ShareID

Peut-on contrer l'IA par l'IA ?

Face à cette menace, des solutions « AI vs AI » émergent. Elles reposent sur l'entraînement d'IA défensives capables de détecter les signatures laissées par des documents générés artificiellement : incohérences dans les métadonnées, anomalies statistiques, empreintes numériques. Shift Technology, par exemple, expérimente des modules de détection de faux documents intégrés à ses systèmes d'analyse (Shift Technology).

CHIFFRES CLÉS À RETENIR

- **+700 %** d'augmentation des tentatives de fraude par deepfake en France en un an
- **+281 %** d'usage de documents d'identité synthétiques détectés en 2024
- Plus de **13 M€ de fraudes stoppées par l'Assurance Maladie** grâce au dispositif ASAFO-Pharma, avec **7 300 suspicions** recensées et **75 % confirmées**
- Le dark web enregistre **2,5 Millions de visites par jour en 2023**, en hausse à **2,7 Millions au printemps 2023**
- **8,4 utilisateurs sur 1 000** cliquaient chaque mois sur un lien de phishing en 2025, contre 2,9 en 2023
- En 2023, la CNAM a démantelé un réseau de **sept centres de santé impliqués** dans des pratiques frauduleuses coordonnées, entraînant déconventionnements et plaintes pénales

5. PROFESSIONNELS DE SANTÉ ET ASSURANCE : ENTRE CONFIANCE ET SURVEILLANCE MUTUELLE ?

La lutte contre la fraude santé ne concerne pas uniquement les assurés ou les fraudeurs organisés ; elle touche aussi directement les professionnels de santé. Leur rôle est à la fois central et ambigu : certains deviennent malgré eux les complices d'irrégularités, tandis que d'autres sont injustement soupçonnés en raison des signaux faibles détectés par les algorithmes. Dans ce contexte, l'équilibre entre contrôle et confiance est devenu un enjeu majeur pour maintenir une relation apaisée entre soignants et assureurs.

Des soignants : complices ou victimes ?

L'explosion des fraudes via ordonnances falsifiées et téléconsultations fictives place également de nombreux praticiens dans des situations complexes. Certains sont instrumentalisés malgré eux, lorsque des patients présentent des documents frauduleux générés par IA — souvent sans que les soignants ne s'en rendent compte — ou voient leur numéro Adeli utilisées à leur insu pour des facturations illégitimes.

D'autres cas relèvent toutefois de complicités actives : c'est le cas de sept centres de santé ophtalmologique du réseau Ophtalmologie Express, déconventionnés en avril 2025 pour des pratiques frauduleuses délibérées. Opérant dans cinq départements (Bourgogne-Franche-Comté, Grand-Est, Bretagne, Île-de-France, Normandie), ces centres ont été sanctionnés suite à la détection de **facturations d'actes non réalisés**, des actes facturés **sans la présence d'un ophtalmologue ou d'un orthoptiste**, ou encore des facturations « sur consigne », sans lien avec l'état de santé des patients. Ces faits ont été révélés après le déploiement, en début 2024, d'une task force nationale suite à des signalements relevés sur treize centres du réseau. Le **préjudice total estimé s'élève à 6,6 M€** (Ameli).

Quand l'IA protège aussi les soignants

Paradoxalement, l'IA ne se limite pas à un rôle de contrôle ; elle peut aussi devenir un outil de protection.

- Les alertes automatiques aident les praticiens à repérer des prescriptions potentiellement frauduleuses ou répétitives.
- Des signaux sur des erreurs récurrentes peuvent éviter des sanctions ultérieures, en permettant une correction rapide.
- Les plateformes comme ASAFO-Pharma intègrent désormais des retours en temps réel pour informer les pharmaciens lorsqu'une ordonnance suspecte est identifiée (Ameli).

Ce rôle « préventif » de l'IA contribue à renforcer la sécurité juridique et financière des soignants, tout en consolidant la chaîne de confiance avec les patients et les assureurs.

Préserver la confiance dans un contexte automatisé

Le défi est désormais d'éviter que la lutte contre la fraude ne se traduise par une défiance généralisée. Certains experts soulignent trois conditions essentielles :

- **La transparence des algorithmes**, afin que les soignants comprennent pourquoi ils sont signalés
- **L'accompagnement pédagogique**, avec formation et communication claire sur les outils utilisés
- **La supervision humaine systématique**, garantissant que l'IA reste une aide et non un juge.

Cet équilibre conditionnera la capacité à maintenir un climat de coopération plutôt que de confrontation.

6. LA FRAUDE EN ASSURANCE SANTÉ ET PRÉ-VOYANCE), LES RÉPONSES DES PROFESSIONNELS DE L'ASSURANCE

La fraude en assurance santé : un défi croissant qui mobilise les acteurs du secteur. La rédaction de L'Assurance en Mouvement (Vovoxx Média) a interrogé 102 professionnels de l'assurance santé, du 15 au 19 septembre 2025, pour recueillir leur perception des enjeux liés à la fraude. Les résultats mettent en évidence une préoccupation largement partagée, mais aussi des pistes concrètes d'action pour y faire face.

L'enquête révèle un double constat : la fraude en assurance santé est désormais perçue comme une menace systémique, mais les professionnels gardent la conviction qu'elle peut être contenue. L'avenir passera par un équilibre entre expertise humaine et outils technologiques, adossé à une coopération renforcée, si elle est possible..., entre acteurs privés et publics.

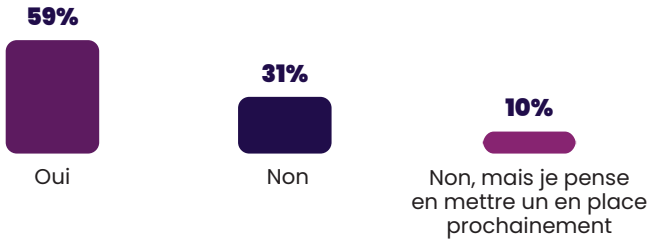
Il y a-t-il des enjeux sur l'évolution de la fraude en santé, pour les acteurs de l'assurance santé dans les années à venir ?

- Enjeux faibles : **7%**
- Enjeux importants : **91%**
- Je ne sais pas : **2%**

Si les enjeux sont importants, sur quels types de garanties en particulier ? (3 réponses maxi)

- Optique : **90%**
- Dentaire : **70%**
- Arrêt de travail : **70%**
- Pharmacie : **30%**
- Hospitalisation : **10%**
- Autre(s) : **10%**

Utilisez-vous un dispositif anti-fraude actuellement (sur l'assurance santé) ?



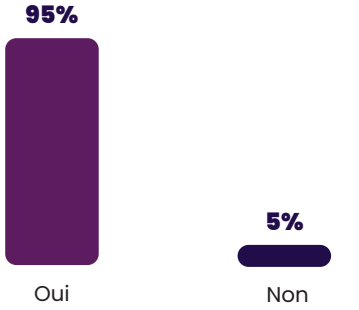
Si oui (question précédente), votre dispositif actuel de lutte contre la fraude (sur l'assurance santé) est-il :

- Uniquement fait manuellement (Humain) : **29%**
- Uniquement fait grâce à des traitements automatisés : **14%**
- Les deux (Traitements automatisés + Humain) : **57%**
- Autre… : **0%**

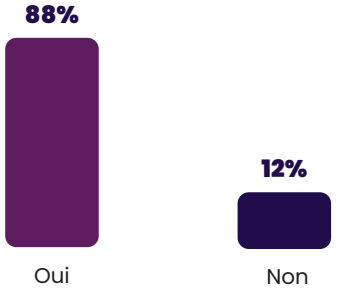
Concernant l'utilisation de l'intelligence artificielle actuellement pour lutter contre la fraude à l'assurance santé, qu'en pensez-vous ?

- Elle est indispensable : **77%**
- Elle est utile : **23%**
- Elle ne présente pas d'intérêt : **0%**
- Je ne sais pas : **0%**

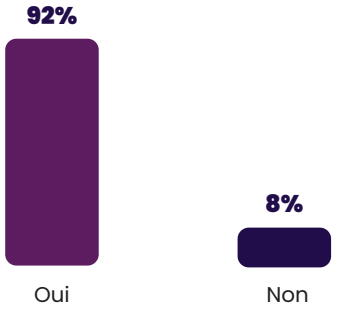
Selon vous, devrait-il y avoir des ponts de collaboration avec les assurances santé et l'Assurance Maladie, pour une gestion coordonnée de la fraude santé ?



Voyez-vous émerger de nouvelles menaces (deepfake de documents, IA générative, ….) dans le domaine de la fraude à l'assurance santé ?



La fraude à l'assurance santé peut-elle vraiment être réduite ?



Si oui, Comment ?

- Mobilisation des assureurs auprès des professionnels de santé
- Par des technologies de pointe efficace et des incohérences des fraudeurs et récurrence.
- En augmentant moyens humains et financiers, collaboration entre tous les acteurs
- Analyser toute la chaine de soins et pas seulement une demande spécifique.
- Intensifier la collaboration de tous les acteurs (RO, RC…)
- Grace a une entraide entre les différents acteurs, un partage des fraudes identifiées par chacun pour créer une base antifraude commune
- Enquêteurs

Pour terminer, quelles innovations techniques ou réglementaires pourraient faire progresser la lutte contre la fraude à l'assurance santé dans les 3 à 5 ans ?

- Informatique quantique
- IA, contrôle, tracking des fraudeurs réguliers par les réseaux sociaux.
- Contrôle des prescriptions avec QR code, autoriser échanges entre RO et OC
- Plus D'IA et de coopérations entre les différents services publics et privés

7. VERS UNE IA RESPONSABLE ET DÉFENSIVE ?

Si l'intelligence artificielle s'impose comme un levier stratégique pour lutter contre la fraude santé, elle ouvre aussi de nouveaux défis : celui d'une gouvernance responsable et celui d'une contre-offensive face à l'usage malveillant de la technologie par les fraudeurs. Les prochaines années verront sans doute émerger des IA dites « défensives », conçues pour identifier et neutraliser des fraudes générées par d'autres IA.

Besoin d'IA défensives

La multiplication des deepfakes médicaux et des faux justificatifs générés par IA impose aux assureurs et institutions publiques de renforcer leur arsenal. Les solutions traditionnelles de détection ne suffisent plus face à des documents artificiels quasi indétectables.
Des initiatives comme celle de ASAFO-Pharma, qui a permis en 2024 de détecter **plus de 7 300 ordonnances suspectes** pour un préjudice évité de 13 M€, illustrent l'efficacité de systèmes spécialisés, mais ces dispositifs doivent désormais intégrer des modules capables d'identifier les signatures laissées par des IA malveillantes (Ameli).

Transparence et supervision humaine

Le cadre réglementaire fixe déjà des obligations fortes, pour rappel :

- Le **RGPD** impose la traçabilité et la notification des incidents dans les 72 heures (Source : **CNIL**).
- L'**IA Act**, entré en vigueur en août 2024, classe les systèmes d'IA appliqués à la santé comme des outils « à haut risque », avec des obligations de transparence algorithmique, de supervision humaine et d'auditabilité.
- **La CNIL et l'ANSSI** rappellent que les décisions automatisées ne peuvent avoir d'impact direct sur un assuré ou un professionnel de santé sans validation humaine (Source : **CNIL**).

Ces garde-fous visent à éviter que l'IA ne devienne un « juge » opaque, tout en rassurant les soignants et les assurés sur l'équité des contrôles.

L'émergence d'un modèle « AI vs AI »

Les laboratoires de recherche et les acteurs privés testent désormais des systèmes « AI vs AI », où des intelligences artificielles défensives sont entraînées pour reconnaître les traces laissées par des IA génératives utilisées à des fins frauduleuses.
Par exemple, Shift Technology développe des algorithmes capables de comparer des ordonnances à de vastes bases de documents authentiques afin de repérer les incohérences statistiques ou les anomalies visuelles (Shift Technology).
Ces outils ne se substituent pas aux experts humains ; ils offrent un niveau supplémentaire de vigilance dans un contexte où la fraude devient de plus en plus automatisée et difficile à détecter.

Un équilibre encore fragile

Si ces innovations renforcent les défenses, elles posent de nouvelles questions : comment garantir l'indépendance des IA défensives ? Qui en assure la gouvernance ? Et comment éviter une escalade technologique entre fraudeurs et assureurs ? Les réponses dépendront autant des choix réglementaires européens que de la capacité des acteurs publics et privés à coopérer.

8. FRAUDE À L'ASSURANCE SANTÉ : VERS UNE OPTIMISATION DE LA COOPÉRATION PUBLIC–PRIVÉ ?

La lutte contre la fraude santé dépasse largement la capacité d'un acteur isolé. La CNAM comme les organismes complémentaires (AMC) s'accordent sur un point : seule une coordination renforcée offre une réponse efficace face à la sophistication croissante des fraudes : entre ordonnances falsifiées, téléconsultations fictives et surfacturations structurées.

Historique d'une coopération insuffisante

La coopération entre Assurance Maladie obligatoire (AMO) et complémentaires santé (AMC) a longtemps souffert de cloisonnements. Les différences de systèmes d'information, les contraintes juridiques liées au RGPD et la crainte d'exposer des données sensibles ont limité la circulation d'informations.
Pourtant, la fraude n'épargne aucun périmètre : les complémentaires sont régulièrement confrontées à des dossiers déjà suspects dans le régime obligatoire. Ce manque de fluidité engendre des doublons dans les contrôles et laisse des marges aux fraudeurs.

Le retour du sujet au Parlement ?

Le **13 mai 2025**, une proposition de loi portée par le député **Cyrille Isaac-Sibille** a été déposée afin d'**institutionnaliser la coopération entre AMO et AMC dans la détection des fraudes**. Elle reprend intégralement l'esprit de l'article 49 du PLFSS 2025, censuré précédemment par le Conseil constitutionnel, et vise à :

- Autoriser des échanges ciblés d'informations utiles entre caisses et complémentaires,
- Garantir que seules les données strictement nécessaires soient partagées,
- Prévoir des plateformes sécurisées de transmission, conforme à l'avis de la **CNIL.**

Préconisations d'experts indépendants

Le **Haut Conseil pour le Financement de la Protection Sociale (HCFiPS)**, dans un rapport publié en septembre 2024, recommande la mise en place d'un **tiers de confiance juridique** pour piloter et encadrer les échanges entre AMO et AMC. Cette solution permettrait d'assurer transparence, traçabilité et respect du RGPD, sans démanteler les frontières entre systèmes.

Des attentes fortes et des perspectives concrètes

D'après un rapport du Sénat, une coopération améliorée permettrait aux AMC de se voir restituer des indus qui leur échappent aujourd'hui, tout en renforçant la détection rapide des fraudes. Des estimations récentes évoquent des gisements d'économie de l'ordre de 52 M€ pour Malakoff Humanis ou 45 M€ pour Harmonie Mutuelle, faisant dire à leurs dirigeants que des efforts partagés pourraient atteindre une efficience équivalente à celle des régimes obligatoires.

Au-delà des économies financières, cette coopération permettrait aussi une meilleure traçabilité des dossiers et contribuerait à renforcer la confiance des assurés, en réduisant les abus et en réallouant les ressources vers des besoins légitimes.

Des défis persistants

Cette coopération se heurte toutefois à plusieurs obstacles : protection des données, avec la nécessité de garantir le respect du RGPD et des principes de minimisation ; interopérabilité technique, pour unifier des systèmes d'information parfois incompatibles ; et climat de confiance, car il s'agit de convaincre les professionnels et les assurés que la lutte antifraude ne se fait pas au détriment de leurs droits. Les experts soulignent par ailleurs l'importance d'un accompagnement pédagogique et de formations dédiées, afin que les acteurs de terrain comprennent le fonctionnement des dispositifs et ne perçoivent pas ces outils comme une mise sous surveillance généralisée.

En résumé

La coopération AMO–AMC sur la fraude santé est à la fois une **urgence institutionnelle** et une **opportunité stratégique**. Elle promet efficacité, économies, et meilleure qualité de soins — à condition d'être mise en œuvre dans le respect des données, avec des garanties humaines et techniques robustes.

Cyrille Isaac-Sibille
DÉPUTÉ

La proposition de loi n° 1403 vise à instaurer un cadre juridique adapté pour faciliter les échanges ciblés d'informations entre AMO et AMC, tout en garantissant la protection des données. L'objectif est de lever les freins juridiques (notamment liés à la protection des données) qui empêchent aujourd'hui une meilleure coopération entre l'assurance maladie obligatoire (AMO) et les complémentaires santé (AMC) pour la lutte contre la fraude. Elle s'inscrit dans la continuité d'une mesure budgétaire précédemment adoptée puis censurée, avec un objectif clair : améliorer la détection, le suivi judiciaire et le recouvrement des fraudes dans un contexte de pression budgétaire. En 2024, l'Assurance maladie a détecté 628 millions d'Euros de fraudes, un record marquant l'ampleur du renforcement des dispositifs de contrôle, mais aussi l'extension des réseaux organisés. D'après les données de l'Assurance maladie, 52 % des fraudes sont commises par des assurés, pour 18 % des montants, et 27 % des fraudes sont commises par des professionnels de santé, pour 68 % des montants.

Principales dispositions du texte

1. Article 1er – modifications du code de la sécurité sociale (art. L. 114 9 et nouveau L. 114 9 1) : Lorsqu'une caisse d'assurance maladie dépose plainte, elle doit transmettre au procureur les coordonnées des organismes complémentaires concernés et toute information pertinente sur le préjudice subi
En cas de suspicion de fraude, les agents de l'AMO ou de l'AMC peuvent échanger des informations strictement nécessaires à l'enquête, limitées à la nature des actes concernés. Ces données doivent être supprimées si la fraude est infirmée, et leur usage limité à des fins judiciaires ou de contrôle seulement ; un intermédiaire tiers sécurisé doit être utilisé pour ces échanges

2. Article 2 – financement
Le dispositif serait financé notamment par une augmentation de la taxe sur le tabac, selon les modalités habituelles de compensation budgétaire.

Cyrille Isaac Sibille est médecin ORL de formation, ancien maire adjoint de Sainte Foy lès Lyon et député centriste de la 12è circonscription du Rhône (MoDem / groupe Les Démocrates), élu depuis 2017 et réélu en 2022 et 2024. Actif au sein de la Commission des affaires sociales, il se distingue par ses travaux sur la prévention en santé, la promotion de la santé publique, le dossier médical partagé et la lutte contre la pollution aux PFAS, mission confiée en 2023 par le Gouvernement. **Cyrille Isaac-Sibille a déposé une proposition de loi « visant à améliorer la coordination entre l'assurance maladie et les complémentaires santé dans la lutte contre la fraude**. Il répond à nos questions (Interview réalisé le 30 juillet 2025).

La lutte contre la fraude (assurance santé) est-elle une priorité politique ?

La lutte contre la fraude est une priorité politique, qui s'est accentuée ces dernières années. Jusqu'à présent, elle a plutôt fait l'objet de mesures ponctuelles, éparses, inscrites dans les différents textes budgétaires.

J'ai moi-même déposé en mai dernier une proposition de loi reprenant une mesure écartée de la loi de financement de la Sécurité sociale, visant à renforcer la coopération de l'Assurance maladie et des complémentaires santé dans la lutte contre la fraude. Je suis confiant quant à l'intégration de cette mesure dans le futur projet de loi que présentera le Gouvernement cet automne.

Conscient de l'importance de la fraude, le Gouvernement a annoncé la présentation d'un projet de loi dédié à la lutte contre la fraude sociale et fiscale, examiné en novembre prochain, en parallèle de l'examen budgétaire. L'objectif est de récupérer 15 milliards d'Euros.

Le financement via une hausse de la taxe sur le tabac est-il la seule piste envisagée ?

Dans cette proposition de loi, nous avons prévu un gage sur la fiscalité du tabac afin de compenser la perte de recettes que pourrait engendrer la mise en œuvre de la coopération entre l'Assurance maladie obligatoire et les complémentaires santé. Ce gage est une exigence technique qui permet de garantir la recevabilité financière du texte, conformément aux règles de la procédure parlementaire, et qui ne préjuge pas du mode de financement réel de la mesure. Ce gage sera levé par le Gouvernement à l'issue de l'examen de la proposition de loi.

Quel est le coût global estimé pour les organismes concernés (AMO/AMC et prestataires intermédiaires) ?

Le coût de mise en œuvre de cette mesure (mise à jour des systèmes d'information, organisation du croisement des données, …) est négligeable à long terme, au regard des recouvrements et amendes significatifs qu'elle permettra

de réaliser. Tant du côté de l'Assurance maladie que des acteurs privés, il y a un consensus pour dire que cet investissement est justifié et nécessaire.

Voyez-vous encore des obstacles juridiques pour une coopération AMO/AMC efficace aujourd'hui ? Comment sera précisée la liste des informations échangées ?

Le principal frein est le manque de confiance entre ces organismes.
La liste des informations échangées sera précisée par décret. Seules les informations strictement nécessaires à l'identification de l'auteur des faits de fraude suspectés pourront être échangées, dans le strict respect du RGPD et après avis de la CNIL.

Sur quels types de fraude ce dispositif permettra-t-il de porter une action plus rapide et plus directe ? Prévoyez-vous un effet dissuasif chez les fraudeurs, ou une amélioration significative de la détection et du recouvrement ?

Il s'agit en priorité de cibler les fraudes à l'acte fictif (acte facturé mais non réalisé), la surfacturation ou la double facturation entre AMO et AMC, la fraude au tiers payant, notamment en pharmacie ; pour l'optique et les appareils auditifs. Ce croisement des données aura un double effet vertueux : une amélioration concrète de la détection des fraudes et un effet préventif, dissuasif.

Cependant, nous devons, en parallèle, faire une distinction entre l'erreur de bonne foi (souvent lié à la complexité des règles et des formulaires) et la fraude délibérée. Il est essentiel que cette distinction soit inscrite dans la loi et dans le régime des pénalités.

Le texte dans sa configuration actuelle garantit-il la protection du secret médical et des données sensibles ?

Tout à fait. Le texte prévoit que seules les informations strictement nécessaires à l'identification de l'auteur des faits de fraude suspectés pourront être communiquées par l'assurance maladie à la complémentaire santé, et celle-ci ne pourra pas conserver ces données au-delà d'une durée strictement nécessaire afin d'agir en justice ; et réciproquement. Les données échangées, qui transiteront par un intermédiaire présentant un haut niveau de sécurité, ne pourront être utilisées qu'à des fins de lutte contre la fraude sous peine de sanctions pénales et devront être supprimées sans délai si la suspicion est levée.

Cette proposition de loi est-elle suffisante pour optimiser la coordination public/privé sur ces questions de fraude ?

Cette proposition de loi est une première étape, mais pas une fin en soi. L'optimisation de la coordination public/privé nécessite d'actionner d'autres leviers (ex. : outils de détection partagés), mais surtout de développer une confiance entre les acteurs.

Ce texte a vocation à s'inscrire dans un cadre plus large, avec des mesures complémentaires pour lutter contre la fraude sociale.

Vous évoquiez récemment « Il faut que l'Assurance-maladie et les complémentaires se fassent confiance », c'est loin d'être le cas actuellement ? Pourtant il semble y avoir de nombreux « intérêts » partagés, bien sûr sur la fraude en assurance santé, mais aussi sur des sujets comme la prévention, non ?

Nous ne sommes encore qu'aux prémices d'une coordination systémique entre l'Assurance maladie obligatoire et les complémentaires santé.

Le double système de remboursement est devenu complexe et entraîne des inégalités. Depuis quatre ans, nous avons commencé à réformer ce système grâce à la mise en place de la réforme 100% santé (zéro reste à charge). Les mutuelles peuvent être les acteurs moteurs de la prise en charge de la prévention santé et il convient de réfléchir au partage de compétences entre l'assurance maladie et les complémentaires santé, déléguant plus fortement à ces dernières le volet préventif. Aujourd'hui, les complémentaires santé sont cantonnées à un rôle de financeur, alors qu'elles pourraient jouer un véritable rôle en faveur de la prévention en santé. Elles disposent d'un lien direct avec les assurés, d'une connaissance de leurs besoins et parfois de leur environnement. Cette proximité est sous-exploitée alors qu'elle permettrait le déploiement d'actions de prévention ciblées.

Quel calendrier législatif anticipez-vous pour la discussion et le vote de cette proposition ? Quels sont les soutiens politiques (parlementaires, associations, institutions du secteur de l'assurance – Mutualité Française, CTIP, France Assureurs, plateformes santé,....) mobilisés autour de ce projet de Loi ? Les acteurs du privé vous semblent-ils assez actifs sur le sujet ? Etes-vous optimiste sur le vote de cette proposition de Loi ?

Avant les annonces du Gouvernement, nous envisagions de présenter cette proposition de loi dans le cadre d'une semaine transpartisane à l'Assemblée nationale, au mois de décembre.

Les nouvelles annonces du Premier ministre permettent désormais d'envisager son intégration directe dans le projet de loi examiné en novembre prochain, ce qui renforcerait sa portée. Je suis en contact régulier avec le Gouvernement depuis cette annonce.

Je suis optimiste quant à son adoption, pour plusieurs raisons :

- Cette mesure a déjà été adoptée dans le cadre du précédent budget, avant d'être censurée pour des raisons de procédure (car jugée sans lien direct avec le texte budgétaire).

- Elle bénéficie d'un soutien transpartisan, à la fois à l'Assemblée nationale et au Sénat.
- Les acteurs concernés (Assurance maladie et acteurs privés) sont engagés et actifs sur le sujet. Je mène des échanges réguliers avec eux pour construire un dispositif qui répondent aux besoins de chacun.

L'intelligence artificielle est un nouvel outil à disposition pour la détection de la fraude. Paradoxe, L'IA est vigile, mais aussi complice de la fraude, l'intelligence artificielle générative est aussi un outil à disposition de fraudeurs très organisés. Les acteurs publics/privés de l'assurance santé en France ne sont-ils qu'au début d'un véritable défi visant à faire face à une augmentation massive de la fraude (assurance santé) ?

L'intelligence artificielle est un formidable outil, qui permet de détecter plus rapidement et plus efficacement les fraudes, ainsi que les schémas de fraudes. Cependant, les réseaux de fraudeurs utilisent également ces technologies (production de faux documents, usurpation d'identité, ...). Nous sommes donc engagés dans une course technologique, qui rend nécessaire la coordination des acteurs, des moyens et des données, la mutualisation des efforts entre acteurs publics et privés, mais surtout un encadrement des usages de cette intelligence artificielle.

POSTFACE

La lutte contre la fraude en assurance santé entre dans une ère charnière. L'intelligence artificielle ouvre des perspectives inédites : détection en temps réel, analyse de volumes massifs de données, anticipation de schémas frauduleux. Ces avancées renforcent l'efficacité des dispositifs existants et offrent un véritable levier pour protéger la soutenabilité financière du système de santé, tout en préservant la confiance des assurés et des professionnels.

Mais cette même technologie, accessible et puissante, constitue aussi un risque accru : les fraudeurs s'approprient rapidement les outils d'IA, industrialisent leurs pratiques et exploitent les failles d'un écosystème encore fragmenté. La course entre IA défensive et IA offensive ne fait que commencer, et elle impose une vigilance permanente.

C'est dans cette tension que réside les enjeux à venir :

- Construire un modèle équilibré, où l'innovation technique se conjugue à la supervision humaine, et où l'éthique et la transparence deviennent indissociables de la performance.

- Construire la coopération entre acteurs – assureurs, pouvoirs publics, professionnels de santé – qui apparaît alors comme la condition sine qua non d'une lutte antifraude réellement efficace.

Optimisme et lucidité doivent guider l'action : l'IA ne saurait tout résoudre seule, mais elle offre aux acteurs du secteur l'opportunité d'unir leurs forces pour faire reculer la fraude. La réussite dépendra moins de la sophistication des outils que de la capacité collective à bâtir une confiance durable et un cadre de collaboration solide, à la hauteur des défis à venir.

Une production Vovoxx Média • 07/10/2025

MÉDIA

VOVOXX