Le piège de l’Espace Santé de l’assurance-maladie

[Publié initialement sur profession-gendarme.com]

Par le Dr **Gérard Delépine**, chirurgien cancérologue et assuré soci

Dans sa volonté de ficher l'ensemble des Français, le gouvernement vient de lancer l'opération « votre espace santé » en prétendant qu'il permettrait d'être « *soigné plus efficacement* » et que « *La confidentialité des informations du dossier médical* serait *totalement garantie ».* Deux affirmations fausses.

Les précédentes tentatives de « dossier médical partagé » (DMP) ont déjà coûté très cher aux Français

Depuis 18 ans, les tentatives d'imposer le « dossier médical partagé » numérique ont été des échecs retentissants. Lancé en 2004 par les ministres, Philippe Douste-Blazy, relancé en 2008 par Roselyne Bachelot, il avait déjà coûté 500 millions d'euros en 2014[1] pour seulement 418 011 dossiers médicaux ouverts au lieu des 5 millions de DMP prévus – le contrat signé avec la société Santeos.

En 2018, l'arrivée d'E. Macron au pouvoir a été marquée par la relance maximale du tout numérique et singulièrement du projet DMP [2], avec l'inclusion automatique des données de la sécurité sociale dans « mon espace santé » **créé sans accord préalable des intéressés**. Les pharmaciens et les infirmiers sont censés inciter les assurés à l'accepter. Les médecins généralistes sont, quant à eux, financièrement intéressés à alimenter les dossiers[3]. On ne connaît pas encore le coût de ce nouveau fichage, mais il s'annonce très élevé. Ne serait-il pas plus judicieux de consacrer cet argent à la remise en état de nos hôpitaux tant en personnel qu'en matériel et réhabilitation ?

« L’espace santé » ne peut pas améliorer la qualité des soins

Premier mensonge

La qualité des soins repose sur le contact direct (en chair et en os et non pas seulement virtuel, visuel), médecin-malade, le dialogue confidentiel et librement consenti, le nombre et la disponibilité des soignants et surtout leur liberté des choix thérapeutiques, enfin l’état des établissements d’hospitalisation.

Depuis de nombreuses années et tout particulièrement ces deux dernières années, les médecins traitants ont été marginalisés par le pouvoir [4] et se sont malheureusement soumis pour trop d’entre eux aux ukases du pouvoir exécutif. De nombreux lits ont été fermés [5] [6] y compris durant la crise covid. Les soignants ont été harcelés et démotivés d’où de très nombreuses démissions ; arrêts de travail prolongés en particulier en raison des burn-out. L’obligation vaccinale anti-covid inutile et dangereuse que le ministère leur a imposée a été pour beaucoup la goutte d’eau qui les a contraints à abandonner leur vocation, ne pouvant de plus assumer de se taire sur la réalité de la crise covid et en particulier des injections expérimentales.

Sans lits ouverts ni soignants ni liberté de soigner par les médicaments efficaces connus, on ne peut espérer améliorer la qualité des soins.

PUBLICITÉ REDONDANTE SUR LES MÉDIAS À RÉPÉTITION [7]

La prétention de l’« espace santé » d’améliorer la santé n’est donc qu’un slogan publicitaire inatteignable sans remise à niveau de nos établissements de soins ni remotivation des

soignants. La numérisation qui n'est qu'un outil ne peut en rien améliorer la « qualité » des soins, les informations plus précises pouvant d'ailleurs venir par d'autres canaux, y compris le patient lui-même qui a parfois stocké ses examens sur son téléphone, réalisé de beaux graphiques. Tout cela est gentil, mais n'a jamais aidé la vraie médecine clinique à avancer.

La communication électronique de données médicales souvent aseptisées, codifiées, simplifiées, résumées, ne peut pas remplacer le contact direct, au minimum téléphonique entre le médecin de famille et les autres soignants, si besoin est.

Croire que « *mon espace santé* » permettrait mieux qu'en favorisant le contact humain direct entre soignants de coordonner les soins, de renforcer la sécurité sanitaire, ou de limiter les risques de surmédicalisation, pour réaliser des économies pour l'assurance maladie relève du fantasme manipulateur, mensonger. Ce sont les malades qui décident de consulter les médecins et non l'inverse.

Pour éviter la surmédicalisation, il serait bien plus efficace de limiter drastiquement les reportages médicaux qui sont en réalité trop souvent des publicités pour les nouvelles techniques ou de nouveaux médicaments et des incitations à les consommer, par exemple les appels à dépistage du cancer du sein, de la prostate ou du colon en dépit des mises en garde sur les dangers respectifs de ces techniques. Les dépistages, comme le reste des décisions médicales, doivent se baser sur un interrogatoire et sur un examen clinique précis du patient putatif et n'être prescrits qu'à bon escient et non pour alimenter des machines à cash.[8] [9] [10] Le harcèlement déjà en place pour nous inciter à ces dépistages, comme aux injections que nous recevons de l'assurance maladie est déjà insupportable. Le rôle de la sécurité sociale fondé en 1946 n'était pas de choisir et de décider de nos soins, mais bien de les rembourser. L'assurance maladie n'est pas notre

médecin !

Cette création d'un fichier national regroupant les données médicales des Français témoigne de la volonté d'accélération du virage numérique du gouvernement permettant au pouvoir de financer ses affidés du numérique et d'accéder à toutes les données médicales personnelles des Français.

Des données médicales centralisées ne peuvent pas être sécurisées

Deuxième mensonge

Croire que « *la confidentialité des informations du dossier médical serait totalement garantie* » est en totale contradiction avec la réalité. Personne ne peut assurer la sécurité totale d'un fichier informatique.

Le Pentagone a été piraté à de nombreuses reprises [11] [12] et a même créé un concours du « *meilleur pirate du Pentagone* » [13] pour « *sélectionner et rassembler les talents, la technologie et les procédés du secteur privé pour nous aider à élaborer des solutions plus sûres et complètes pour le département de Défense* ».

1410 Américains ont participé à ce concours et en un mois, ont fourni 1189 rapports, permettant de détecter 138 failles « valides et uniques ». Le meilleur d'entre eux, qui a décelé plusieurs failles, a empoché 15 000 dollars à la grande satisfaction de l'institution[14] d'avoir ainsi réussi à renforcer la sécurité à moindre coût. « Si nous avions utilisé la procédure classique, *cela nous aurait coûté plus d'un million de dollars.* »

De même, le FBI, la CIA et les autres agences de sécurité américaine ont été piratés[15] [16] [17].

LE PIRATAGE DES DONNÉES DE SANTÉ : UN MARCHÉ JUTEUX

Les données médicales de l'assurance maladie américaine n'ont pas échappé aux pirates et 9,3 millions de dossiers d'assurance maladie de patients américains ont été mis en vente pour 750 bitcoins, soit environ près de 500 000 euros[18]. Les informations comprennent les noms, adresses courriel, numéros de téléphone, dates de naissance et numéros de sécurité sociale.

Croire que la France est capable d'assurer la sécurité de ses fichiers informatiques est un mirage. Le service des impôts a vu 2000 dossiers personnels sensibles dérobés[19]. Le service France Connect interface avec la sécurité sociale a dû être interrompu après un piratage récent [20].

Fin août 2021, c'est un listing de 700 000 noms, adresses et numéro de Sécurité sociale qui a été volé sur le site Francetest permettant aux pharmacies de transmettre les résultats des tests antigéniques.

Les hôpitaux français sont incapables d'assurer leur cybersécurité

En 2020, Cédric O, le secrétaire d'État à la transition numérique avait recensé ***27 cyberattaques « majeures » contre les hôpitaux***, et entre autres celle contre l'AP-HP (maître d'œuvre du fichier SI-Dep pour le compte du ministère des Solidarités et de la Santé), qui a abouti à la publication sur le Dark Web d'environ 1,4 million de données personnelles de patients ayant été testés pour la COVID-19 [21], listing qui aurait pu être monnayé près d'un million d'euros au marché

noir [22].

Tout récemment, en août 2022, la vulnérabilité des données médicales a été à nouveau illustrée par la cyberattaque contre le Centre hospitalier Sud Francilien[23] de Corbeil-Essonnes qui s'est soldé par de graves perturbations de fonctionnement et la vente sur internet des données personnelles des malades.

> *« Les hackers responsables de la cyberattaque contre le Centre hospitalier sud-francilien de Corbeil-Essonnes, le 21 août dernier, ont mis leurs menaces à exécution. Si l'hôpital ne payait pas la rançon exigée en temps et en heure – d'abord 10 millions de dollars, aujourd'hui cinq à dix fois moins – ils allaient publier une série de données détournées. "Une première diffusion a été orchestrée sous la forme d'un fichier compacté de 11,7 gigaoctets (…) vendredi 23 septembre à 9 h 42, heure UTC exactement", confirme Damien Bancal, responsable du site Zataz.com qui recense les cyberattaques dans le monde. Le spécialiste a vu les informations diffusées par les pirates sur le Darknet, mais a laissé la direction générale du CHSF, qui assure la couverture sanitaire de près de 700 000 habitants de la grande couronne au sud de Paris, confirmer leur réalité. »*

Les médecins et soignants de l'hôpital de Corbeil, déjà en manque énorme de personnel, sont très gênés par cette attaque, d'autant que depuis le mythe du « tout numérique » à l'hôpital, nous manquons cruellement de dossiers papier.

L'assurance maladie n'est malheureusement pas une forteresse numérique

Le 17 mars 2022, près de 510 000 personnes affiliées à l'assurance maladie ont été victimes du vol de données

stockées par l'organisme[24].

La promesse que « *La confidentialité des informations du dossier médical serait totalement garantie* » n'engage donc que ceux qui y croient et s'exposent ainsi à des risques considérables comme des chantages sur leur vie personnelle et familiale et des usurpations d'identité.

La perte du secret médical peut gravement vous nuire

Le secret médical constitue un des piliers de l'acte médical. Lui seul permet la confiance du malade qui peut ainsi exposer sans crainte au médecin ses problèmes les plus intimes « *qui ne sortiront pas du cabinet* ».

« Mon espace santé » crée une brèche de sécurité béante dans ce secret. D'autant que vos données médicales intéressent beaucoup de nombreux organismes (assurances, banque, professionnel du viager) et des individus moins recommandables prêts à payer pour obtenir ces informations. Ils pourraient alors vous faire chanter ou nuire à votre réputation en révélant que vous souffrez du sida, que votre fille prend la pilule depuis ses onze ans, que votre femme souffre de tuberculose ou de problèmes psychiatriques, que votre fils est autiste, mongolien, homosexuel ou transgenre…

Le secret médical mérite d'être bien gardé et c'est absolument impossible s'il est conservé dans un fichier informatisé centralisé.

« Mon espace santé » vous expose aussi à l'usurpation d'identité

En plus de vos données médicales, « Mon espace santé » comporte aussi votre date de naissance, votre adresse, votre

numéro de sécurité sociale octroyé à vie, votre numéro de téléphone, votre adresse internet et vos coordonnées bancaires, toutes données utiles pour une usurpation d'identité. Les victimes du piratage de leur espace santé sont ainsi exposées à un risque d'usurpation d'identité.

Chaque année, 210 000 Français subissent une usurpation d'identité qui les expose à des détournements d'argent, la contraction d'un prêt frauduleux à leur nom, au détournement de leurs prestations sociales… La victime lésée de ses droits financiers ou en charge de rembourser des montants qu'elle n'a ni perçus, ni utilisés, se retrouve parfois poursuivie par la justice pour des infractions ou des délits qu'elle n'a pas commis.

Outre les problèmes financiers, les victimes subissent des conséquences psychologiques et doivent faire des démarches souvent très longues pour prouver leur identité. Récupérer cette identité est un parcours souvent qualifié « d'enfer » par les victimes qui mettent parfois plusieurs années pour retrouver la pleine jouissance de leur identité.[25]

Le marché des données personnelles est un marché en pleine explosion sur le Dark Web.[26] Des zones très spécifiques sont même créées pour permettre aux cybercriminels de faire leurs échanges (de l'ordre de 500 euros pour une carte d'identité ou un permis de conduire[27]). Il y a là de quoi motiver sérieusement les pirates du net, surtout s'ils parviennent à collecter plusieurs millions de données. Le risque est désormais que des escrocs utilisent les données accessibles pour monter de nouvelles attaques ciblées, en utilisant les informations personnelles à leur disposition pour capter la confiance de la victime.

Mesures de sécurité conseillées par les responsables de l'hôpital de Corbeil Évry récemment piraté

Les attaquants vont par exemple rechercher « des patrons, des personnalités importantes », et monter des arnaques comme « les fraudes au président », où l'escroc arrive à obtenir un virement bancaire d'une institution en se faisant passer pour son dirigeant ou son directeur financier, a expliqué Damien Bancal.

Les attaquants peuvent aussi utiliser les numéros de téléphone pour monter les arnaques aux comptes personnels de formation (CPF) ou aux cryptomonnaies, les adresses mail pour faire du « hameçonnage » (en anglais « phishing », inciter l'internaute à télécharger des fichiers malveillants ou à cliquer sur des liens pour lui extorquer des identifiants et codes d'accès).

Nous recevons très fréquemment des appels téléphoniques et de multiples SMS pour nous inviter à profiter de nos comptes formation. Or retraités depuis de nombreuses années, ces appels ne peuvent correspondre qu'à des vols de données. Idem en ce qui concerne les arnaques à la carte vitale. Régulièrement nous recevons des SMS nous disant que notre carte vitale n'est plus valable et nous invitant à donner toutes sortes d'informations pour la récupérer. Méfiance. Ne jamais répondre directement. En cas de doute, joignez directement votre caisse d'assurance maladie et directement par un contact humain.

La preuve en un clic : taper Ameli.Fr

Attention aux SMS, appels ou courriels frauduleux 31 août 2022[28]

EN RÉSUMÉ, IL FAUT REFUSER « MON ESPACE SANTÉ » qui menace votre secret médical et votre sécurité financière

La création de « mon espace santé » est réalisé automatiquement sans que l'accord de l'intéressé n'ait été demandé. En l'espèce, pour ficher un maximum de Français, le gouvernement applique le principe de la vente forcée « qui ne dit mot consent ».

Si vous voulez que votre secret médical soit réellement protégé et que vos données personnelles ne soient pas vendues un jour prochain sur le Darknet, **vous devez faire la démarche de le refuser manuellement.**

Pour ce faire, munissez-vous de votre carte vitale. Rendez-vous tout d'abord sur le site officiel à cette adresse : https://www.monespacesante.fr/enrolement-accueil.

Si vous n'avez pas reçu par lettre un code provisoire, il faut l'obtenir en cliquant sur « générer un code provisoire ». Vous allez recevoir ce code valable pour une durée de six semaines, par mail ou par SMS.

Entrez ce code sur le site, et cliquez sur « **refuser l'activation de mon espace santé** » et n'oubliez pas de télécharger le document d'attestation de refus.

En guise d'alternative, vous pouvez aussi refuser Mon Espace Santé par téléphone au 3422. Là encore, munissez-vous de patience et de votre carte vitale.

PROTÉGEZ-VOUS !

1 https://www.lemonde.fr/sante/article/2014/01/04/dossier-medical-partage-un-cout-excessif-pour-un-succes-mitige_4342961_1651302.html2 https://www.lesechos.fr/idees-debats/editos-analyses/dmp-les-conditions-du-succes-1452163 https://www.lemonde.fr/economie/article/2022/02/03/mon-espace-sante-le-retour-du-dossier-medical-partage-apres-une-serie-d-echecs_6112155_3234.html4 Depuis la recommandation ministérielle « *en cas de suspicion covid n'allez pas voir votre médecin* »5 d'après la DREES depuis fin 2013, 30.000 lits d'hospitalisation ont été supprimés6 4316 lits d'hospitalisation complète fermés en 2021 ET 4900 supprimés en 2020 selon la DREES rapportés par bfmtv.com7 Payée par nos impôts et vos cotisations assurance maladie8 Les cancers du sein causés par les mammographies en quelques liens (linkedin.com)9 Dépistage du cancer de la prostate : le grand mensonge (jeremie-mercier.com)10 Les dépistages des cancers sont-ils aussi utiles que l'on nous les présente ? – Docteur Nicole Delépine (nicoledelepine.fr)
11 https://www.funinformatique.com/prouesses-des-hackers-3-pirates-informatiques-celebres-a-la-loupe/

12 https://www.lefigaro.fr/international/2006/05/11/01003-20060511ARTWWW90372-pour_avoir_pirate_un_serveur_du_pentagone_il_risque_ans_de_prison.php

13 https://www.slate.fr/story/114923/gouvernement-americain-pirates-hackeurs-pentagone

14 https://www.solutions-numeriques.com/securite/docapost-protege-ses-milliers-de-donnees-sensibles/

15 https://www.coupsfrancs.com/un-africain-pirate-le-systeme-informatique-du-fbi-et-de-la-cia-et-distribue-la-nationalite-americaine/

16 https://www.francetvinfo.fr/monde/usa/la-cia-admet-le-piratage-embarrassant-d-emails-personnels-de-son-directeur_1139509.html

17 https://www.20minutes.fr/high-tech/1725211-20151106-jeunes-hackers-cia-recidivent

18 https://www.silicon.fr/10-millions-donnees-sante-dark-web-151489.html

19 https://www.capital.fr/economie-politique/impots-des-milliers-de-comptes-fiscaux-pirates-1347835

20 https://www.herault-tribune.com/articles/piratage-le-service-france-connect-suspendu-pour-la-securite-sociale-ou-les-impots/

21 https://www.bfmtv.com/tech/l-ap-hp-victime-d-une-cyberattaque-les-donnees-de-1-4-million-de-personnes-volees_AD-202109150384.html

22 https://www.20minutes.fr/societe/3129455-20210921-piratage-ap-hp-pourquoi-type-donnees-interessent-pirates-informatiques

23 Hôpital de l'Essonne cyberattaque : les hackers ont diffusé des données, par Éric de La Chesnais 24 sept 2022
Ciblés par les hackers, les hôpitaux français malades de leur cybersécurité

24 https://www.ouest-france.fr/societe/cyberattaque/piratage-de-l-assurance-maladie-comment-reagir-si-vous-faites-partie-des-victimes-7698102

25 https://www.lefigaro.fr/assurance/2014/04/04/05005-20140404ARTFIG00219-les-consequences-d-une-usurpation-d-identite.php

26 https://tehtris.com/fr/blog/usurpation-didentite-causes-et-consequences-dune-menace-redoutabl

27 https://fr.finance.yahoo.com/actualites/valent-donn%C3%A9es-dark-web-121735053.html

28

« Les SMS, appels ou courriels (e-mails) frauduleux se

multiplient.

L'Assurance Maladie met à nouveau en garde les assurés et rappelle qu'il ne faut en aucun cas répondre aux demandes faites par ces messages.

Obtenir une attestation de droits, changer de coordonnées, déclarer une naissance… pour réaliser ces démarches et bien d'autres sans risque et rapidement, c'est facile grâce au compte Ameli ! Pour en savoir plus, consulter la rubrique « Compte Ameli : mode d'emploi ».

Comment les reconnaître pour mieux s'en protéger ?

Ces communications par SMS, appels téléphoniques ou courriels usurpent le nom et le logo de l'Assurance Maladie afin de récupérer des données personnelles ou de faire appeler des numéros surtaxés.

Indices pour repérer les fraudes par téléphone

• Lorsque quelques secondes d'attente s'écoulent entre le moment où l'on décroche et le moment où l'interlocuteur parle, ce temps d'attente peut constituer le 1er indice d'une mise en relation avec une plateforme d'appels frauduleux.

• Le fraudeur tente de rassurer l'assuré et de déjouer sa vigilance en utilisant le nom des services publics officiels ou parfois plus globalement des services de l'État avec lesquels il prétend travailler.

• Le fraudeur dit travailler pour « Ameli » ou pour « l'Assurance Maladie » ou pour le « service digitalisation de FranceConnect en lien avec la Sécurité sociale » ou pour « le compte personnel de formation (CPF) ». Il indique vouloir vérifier le compte Ameli ou le compte FranceConnect ou le compte CPF de l'assuré. Il demande à l'assuré s'il a reçu un courriel (ou e-mail) et comme ce dernier répond non, le fraudeur propose alors de renvoyer le courriel. Il indique ne

pouvoir le faire qu'après s'être assuré de la correcte identité de l'assuré et demande l'adresse de messagerie, le numéro de sécurité sociale, le mot de passe du compte Ameli, etc. C'est ainsi que les accès au compte Ameli de l'assuré sont récupérés par le fraudeur, qui peut alors se rendre sur ce compte Ameli pour récupérer les données qui l'intéressent, voire pour modifier des éléments personnels, comme l'adresse mail ou le mot de passe du compte. Le fraudeur peut aussi utiliser les identifiants du compte Ameli pour accéder à des sites comme celui du compte personnel formation grâce à l'authentification par FranceConnect.

• Le fraudeur insiste sur le caractère urgent de la démarche à réaliser.

Indices pour repérer les fraudes par courriel (e-mail) ou par SMS

• L'assuré reçoit un courriel qui propose un service en ligne payant de mise à jour de la carte Vitale (alors que la mise à jour de la carte Vitale est totalement gratuite et peut se faire dans la plupart des pharmacies).

• L'assuré reçoit un SMS qui signale la livraison d'une nouvelle carte Vitale ou annonce qu'un remboursement de l'Assurance Maladie est en attente avec un lien cliquable. » (…)