NOVEMBRE 2021

TRAJECTOIRE e-santé

LE MAGAZINE DES DÉFIS DU NUMÉRIQUE EN SANTÉ

DOSSIER

CYBERSÉCURITÉ
UNE BATAILLE COLLECTIVE POUR UN VIRAGE NUMÉRIQUE RÉUSSI

FEIMA
Fédération des Éditeurs d'Informatique Médicale et paramédicale Ambulatoire

LA PAROLE À...

Jean-Michel Mis,
député de la Loire, membre de la commission des lois, membre du Conseil national du numérique, membre de la Commission supérieure du numérique et des postes.

« LA CYBERSÉCURITÉ EST UN PRÉALABLE AU TOURNANT NUMÉRIQUE DE NOTRE SYSTÈME DE SANTÉ. »

Comment coordonner (plus) efficacement la force de frappe des nombreux acteurs de la cybersécurité déjà mobilisés en santé ?
La cybersécurité est un préalable au tournant numérique de notre système de santé et à la confiance de tous ses acteurs. En 2021, le gouvernement a présenté un plan[1] à hauteur de 350 millions d'euros pour accompagner les hôpitaux dans leurs protections de leurs systèmes d'information. Avec le Ségur de la santé, le choix a été fait d'investir massivement dans la sécurité des systèmes d'information de santé en donnant aux établissements la capacité de mettre en œuvre les outils pour augmenter leur niveau de protection et en apportant des réponses aux incidents. Ces activités portées par l'ANS sont renforcées par la mise en place du CERT-Santé. Appuyé par l'ANSSI, le CERT-Santé joue un rôle essentiel en matière de veille active face aux menaces de cyberattaques. Il permet à tous les acteurs de coopérer afin de leur permettre de monter en compétence et de contribuer, tous ensemble, à une plus grande résilience.

Comment généraliser l'échange et le partage sécurisé des données de santé entre un système numérique national toujours plus interopérable et des « structures » fermées ?
Les systèmes ne s'opposent pas. Il faut poursuivre les investissements pour généraliser l'échange et le partage sécurisé des données de santé, et, malgré l'hétérogénéité des acteurs, s'appuyer sur leurs capacités à s'adapter au changement. Il est aussi crucial de se saisir des politiques de rapprochement et de mutualisation entre établissements de santé, souhaitées par les pouvoirs publics, notamment à travers le plan MaSanté2022, pour renforcer la cyber-résilience de l'ensemble de la chaîne[2]. Il est enfin nécessaire de favoriser la fertilisation croisée entre acteurs des secteurs public et privé en s'appuyant notamment sur nos entreprises émergentes.

1. Stratégie Cyber présentée le 18 février 2021 par le président de la République.
2. « Cybersécurité : accompagner un système de santé en pleine mutation » ; *Renaissance numérique*, février 2020.

CYBERSÉCURITÉ
UNE BATAILLE COLLECTIVE POUR UN VIRAGE NUMÉRIQUE RÉUSSI

De la récente fuite sur les réseaux du QR Code du passe sanitaire du président de la République aux différentes cyberattaques visant les structures de santé, la cybersécurité est au cœur des enjeux de la transition numérique. Avec de nouveaux moyens et un plan de renforcement de la sécurité en santé. Explications…

Dans l'Hexagone comme ailleurs, aucun secteur n'est épargné par les cybermenaces, mais c'est par le biais de la santé et plus particulièrement de l'hôpital que le sujet va s'imposer dans le débat public au début de l'année 2021. Et inciter les pouvoirs publics à lancer une stratégie nationale d'accélération pour la cybersécurité (février 2021).

UN ARSENAL DE DISPOSITIFS POUR LES HÔPITAUX…

Déclinaison pour les établissements hospitaliers de la stratégie nationale pour la cybersécurité, le plan de renforcement de la sécurité en santé s'appuie sur la feuille de route du numérique en santé et le volet numérique du Ségur. À l'échelle nationale, il comprend un observatoire de maturité des systèmes d'information des établissements de santé qui intègre les audits réalisés par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et le CERT-Santé. À l'échelle territoriale, les agences régionales de santé (ARS) ont en charge la sensibilisation des acteurs, le partage des pratiques et l'organisation des réponses aux incidents. Quant aux groupes hospitaliers de territoire (GHT), ils montent en puissance comme accélérateurs des nouveaux usages numériques, organisés autour de la sécurisation des systèmes

Sur la somme attribuée au Ségur,

350 M€

seront dédiés à renforcer la sécurité des systèmes d'information de santé.

d'information partagés, de la mutualisation des moyens cyber et des capacités de réponse aux incidents. Identifiés comme opérateurs de services essentiels (OSE), ils doivent, comme l'ensemble des structures de santé, mettre en œuvre des « règles d'hygiène informatique » élaborées par l'ANSSI et détaillées dans un guide dédié.

… MAIS TRÈS PEU POUR LE SECTEUR AMBULATOIRE DE PREMIER RECOURS

Dans un contexte de déploiement accéléré de services d'échange et de partage d'informations entre acteurs interconnectés, chaque maillon de la chaîne doit faire l'objet d'une attention particulière. Or, force est de constater que peu de leviers d'action ciblent le secteur ambulatoire, dont les acteurs sont pourtant déjà victimes de fuites de données. Plus que jamais, les professionnels de santé doivent donc pouvoir compter sur des experts au savoir-faire et à l'éthique irréprochables pour exercer dans un environnement le plus sûr possible. De longue date, les éditeurs de la FEIMA sont sur le front pour assurer la disponibilité, l'intégrité, la confidentialité et la traçabilité de l'information médicale, dans le respect du cadre législatif et réglementaire. Une mobilisation intégrant la prise en compte des différentes exigences, de la conformité RGPD aux référentiels CNIL en passant par ceux de la Politique générale de sécurité des systèmes d'information de santé (PGSSIS)… Ils se sont par ailleurs récemment impliqués dans la conception des critères éthiques des LGC destinés à enrichir les référentiels de la doctrine technique du numérique en santé, ainsi que dans la validation du « Mémento de sécurité informatique pour les professionnels en exercice libéral » destiné à les accompagner dans les bonnes pratiques en matière de sécurité. Enfin, désireux de poursuivre leur engagement historique sur ces questions fondamentales, les membres de la FEIMA ont adopté lors de leur assemblée générale de septembre 2021 des dispositions, traduites dans **une charte « Engagé pour la cybersécurité »,** visant à renforcer les réponses sécuritaires et éthiques pour le secteur ambulatoire (*voir la rubrique Les actus de la FEIMA*). À bon entendeur !

EN SAVOIR +

TOUS CYBERVIGILANTS

Le ministère de la Santé a lancé en juin dernier la campagne nationale d'information et de sensibilisation 2021 sur les risques numériques en santé. L'objectif ? Inciter tous les acteurs à se mobiliser autour quatre axes : encourager à mieux protéger les outils de travail numérique et les données de santé ; donner les bons réflexes en matière d'hygiène numérique et diffuser les bonnes pratiques ; contribuer à la prise de conscience du rôle de chaque professionnel, de santé ou non, en matière de cybervigilance ; améliorer la connaissance des piliers opérationnels de cybersécurité pour le secteur de la santé, organisés autour du CERT-Santé.

En avril 2021, le CERT-Santé a publié « L'observatoire des signalements d'incidents de sécurité des systèmes d'information pour le secteur de la santé sur l'année 2020 ». Ce document recense les signalements d'incidents cyber des établissements de soins. Les attaques par maliciels (logiciels malveillants) représentent 25 % des incidents déclarés (369 au total), et pour moitié, il s'agit de rançongiciels.

Données de 2020 — Données de 2019

369/392
incidents déclarés sur le portail des signalements

290/300
structures ont déclaré au moins un incident

90/70
demandes d'accompagnement par le CERT-Santé

32/0
interventions pour un appui technique (investigation numérique, remédiation, etc.)[1]

FSSI

7/14
incidents ont fait l'objet d'un suivi particulier de la part du FSSI

ANSSI

14/11
incidents ont été pris en charge par l'ANSSI

ansm
Agence nationale de sécurité du médicament et des produits de santé

4/16
incidents ont été communiqués à l'ANSM

CORRUSS

4/8
incidents ont fait l'objet d'une alerte à la DGS/ CORRUSS

1. Appui pouvant mobiliser un expert pendant plusieurs jours dans l'investigation numérique et la recherche d'indicateurs de compromission.

« LE SECTEUR DE LA SANTÉ N'EST ACTUELLEMENT PAS SPÉCIFIQUEMENT CIBLÉ même si les attaques sont nombreuses et en augmentation, ceci proportionnellement à la multiplication des vulnérabilités inhérentes à la forte transformation numérique. Concernant les rançongiciels et les cyberattaques en général, leur impact sur les structures ou les cabinets dépend essentiellement de leur maturité SSI. Pour l'ambulatoire, nous comptons sur les éditeurs pour qu'ils intègrent au plus tôt les exigences de sécurité dans leurs produits (*security by design*) mais aussi qu'ils prennent en charge ou participent à la prise en charge des recommandations du récent mémento sécurité produit en concertation avec eux, d'autant qu'il y a une interaction très forte entre professionnels de santé et éditeurs. À ce titre, nous regardons de manière approfondie l'émergence, pour les libéraux, d'offres de gestion du cabinet en mode cloud intégrant une surveillance sécurité permanente des applications métiers. »

Jean-François Parguet, fonctionnaire de sécurité des systèmes d'information des ministères sociaux, ministère des Solidarités et de la Santé.

LES ACTUS DE LA FEIMA

ENGAGÉ pour TOUS CYBER VIGILANTS la CYBERSÉCURITÉ

CHARTE « ENGAGÉ POUR LA CYBERSÉCURITÉ »

Initiée par la FEIMA, à destination de ses membres et de tout nouvel industriel adhérent, cette charte fixe les lignes de conduite à respecter pour répondre aux obligations sécuritaires et éthiques à apporter au secteur ambulatoire. Ce document définit aussi les actions de sensibilisation et d'accompagnement à mettre en œuvre auprès des professionnels de santé. Un engagement essentiel qui nécessitera des actions de mise en conformité de leur part et ce au regard de leurs obligations en tant que responsables de traitement des données.

Volet numérique du Ségur : transversalité et simplification des pratiques

Portée par le programme Ségur numérique, la transversalité est un réel vecteur d'optimisation pour les professionnels de santé : amélioration des conditions de travail, fluidité des échanges entre tous les acteurs, enrichissement de la relation patients, atteinte des objectifs de la ROSP dans le calendrier imparti. C'est aussi un levier de soutien vers les éditeurs pour renforcer leurs actions tout au long du processus de mise en œuvre de nouvelles fonctionnalités et solutions. Placer tous les acteurs sur la même ligne de départ, avec les mêmes objectifs techniques, fonctionnels et calendaires est un fait relativement unique dans l'histoire des SI de santé pour qu'il soit souligné !

Sérialisation : des logiciels agréés et prêts à l'emploi pour répondre aux exigences européennes

Avec seulement 233 officines connectées sur plus de 21 000 en mars dernier, la France fait figure de dernier de la classe dans l'application du dispositif de sérialisation entré en vigueur le 9 février 2019 (directive européenne 2011/62/UE). Les éditeurs de la FEIMA rappellent qu'ils ont redéveloppé leurs logiciels pour répondre aux exigences des syndicats français, d'un niveau de complexité supérieur aux autres pays européens. Les pharmaciens peuvent donc répondre à leurs obligations légales.

LA FEIMA EN BREF

La Fédération des Éditeurs d'Informatique Médicale et paramédicale Ambulatoire (FEIMA) représente les éditeurs majeurs du secteur ambulatoire français. Depuis plus de trente ans, les éditeurs membres de la FEIMA conçoivent et développent des offres de logiciels et de services numériques à destination première des professionnels de santé (plus de 80 % des médecins, dentistes, paramédicaux et pharmaciens) et des patients.

Acteurs industriels de premier plan, les membres de la FEIMA constituent un formidable levier de création d'emploi, de valeur et d'innovation sur le marché du numérique en santé, en France et en Europe.

Depuis sa création, en 1996, la FEIMA s'est imposée comme interlocuteur clé des pouvoirs publics et des organisations représentatives des professionnels de santé, dans une démarche coconstructive.

En savoir plus : www.feima.fr

Suivez-nous sur

Conception et réalisation **Comfluence** – Novembre 2021 – Photos : ©iStockphotos – DR – Assemblée nationale

LOGICIELS MÉTIERS LAP ET LAD
UNE CERTIFICATION HAS BASÉE SUR LE VOLONTARIAT

Gage de qualité et de sécurité, la certification atteste la conformité des logiciels métiers avec les critères contenus dans les référentiels définis par la HAS (information sur le patient et le médicament, affichage des médicaments, prescription, sécurité des données…). Dans le cas des logiciels LAP et LAD, la certification est devenue facultative. Cherchez l'erreur…

La procédure de certification par la HAS a été étendue aux logiciels LAP et LAD afin de faciliter leur mise à disposition et d'assurer auprès des prescripteurs et des dispensateurs une meilleure diffusion des informations présentes sur la liste des produits et prestations remboursables (LPP)[1].
Or, une décision de la Cour de justice de l'Union européenne (CJUE) de 2017 et une autre du Conseil d'État (2018) sont venues affaiblir la portée de cette certification : elles précisent que si lesdits logiciels sont qualifiés de dispositifs médicaux, ils doivent faire l'objet d'un marquage CE et ne peuvent se voir imposer en sus la certification de la HAS !

UN RENFORCEMENT DE LA QUALITÉ… SANS PROCESSUS DE CERTIFICATION ?

Dans les faits, la certification HAS de ces logiciels reste possible… mais uniquement sur la base du volontariat ! Désormais facultative, la certification HAS reste cependant complémentaire au marquage CE au titre de dispositif médical. Elle fait d'ailleurs partie des exigences du forfait « Structure » destiné aux médecins (aide annuelle à la modernisation des outils informatiques).
Cette situation de droit est un recul dans la mesure où les exigences liées à la certification sont importantes et continuent à progresser, allant de fait dans le sens du renforcement de la qualité et des obligations des logiciels d'aide à la prescription et à la dispensation (*voir Le saviez-vous ?*).

LA CERTIFICATION, NOUVEAU SACERDOCE ?

En plus de devenir facultative, la certification devient aujourd'hui un obstacle. En effet, si les éditeurs de logiciels s'engagent de manière volontaire dans la voie de la certification, ils encourent des sanctions financières importantes

et inadaptées :

- Le mécanisme de sanction économique appliqué aux logiciels d'aide à la prescription et à la dispensation est une reproduction des sanctions applicables aux dispositifs médicaux soumis à remboursement. Or, les logiciels ne sont pas destinés aux patients, mais aux professionnels et ne sont donc pas remboursés !
- Les logiciels concernés peuvent, dès lors qu'ils sont marqués CE, être commercialisés sans certification et donc sans risque de sanction.

Aujourd'hui, la situation est telle que de nombreux éditeurs font le choix de ne pas certifier leurs logiciels, voire se retirent du processus de certification qu'ils appliquaient jusqu'alors. Or, ces logiciels constituent un outil quotidien très utile pour faciliter les tâches répétitives ou repérer de potentiels risques liés à certaines prescriptions et dispensations. D'ailleurs, la CNAM met en œuvre, dans le cadre de la politique conventionnelle avec les organisations représentatives des professionnels de santé, une rémunération liée à l'usage de ces logiciels certifiés. Dans ce contexte, la FEIMA propose d'adapter les dispositions contraignantes existantes pour un dispositif devenu volontaire et ce afin de renforcer son attractivité. Et de favoriser ainsi le développement d'une certification, gage de sécurité et de qualité pour les patients…

1. Loi du 29/12/2011 relative au renforcement de la sécurité sanitaire du médicament et des produits de santé et rendant obligatoire la certification des LAP, selon un référentiel établi par la Haute Autorité de santé (HAS).

LE SAVIEZ-VOUS ?

Expérimentée depuis 2019 puis appelée à se généraliser en 2022, la e-prescription permet la dématérialisation du circuit de l'ordonnance entre médecin et pharmacien. La e-prescription devrait être étendue aux actes de biologie et paramédicaux en 2022.

Les objectifs des LAP et des LAD :

- **assurer la sécurité des prescriptions et des dispensations (risque d'iatrogénie, d'allergies, d'interaction médicamenteuse, de dépassement de posologie…) ;**
- **améliorer l'efficience des traitements (appartenance d'un produit au répertoire des génériques, coût des produits…) ;**
- **fournir une information complète sur tous les produits ;**
- **faciliter le travail des prescripteurs et des dispensateurs.**

Les LAP et les LAD doivent s'adosser à une base de données médicamenteuse, elle-même certifiée par la HAS et hébergée par la CNAM. Depuis les premiers référentiels publiés par la HAS et bien avant que ce soit obligatoire, les éditeurs de la FEIMA ont intégré toutes ces exigences au sein de leurs solutions. Chaque année, ce sont des millions de prescriptions qui sont ainsi sécurisées grâce à leurs logiciels !