CHARTE

ENGAGE pour TOUS CYBER VIGILANTS
la CYBERSECURITE

1. Le contexte

La santé connait aujourd'hui un formidable essor du numérique. Tout au long du parcours de soins, la donnée de santé est partout : au cabinet, comme à l'hôpital ou au domicile. Une omniprésence qui s'est accrue avec la crise sanitaire.
Lutter contre les déserts médicaux, décloisonner les parcours de soins, désengorger l'hôpital, faciliter la prévention, proposer une nouvelle offre de services ou accélérer la médecine personnalisée... Ces avancées ne pourront se développer que si notre système de santé est capable d'élever le niveau de sécurité de ses données et de ses échanges.

Les cyber-risques sont à l'image de cet essor : ils augmentent. Le secteur de la santé est d'autant plus vulnérable qu'il est chaque jour particulièrement sollicité et sous tension. Stratégiques pour le pays, inégalement matures face au numérique et source exponentielle de données personnelles, les organisations sanitaires constituent une cible privilégiée pour les attaques malveillantes. Avec un impact d'autant plus fort que la santé et la vie des patients sont en jeu.

Le nombre de cyberattaques a explosé depuis le début de l'épidémie de Covid-19. En France, 100.000 infractions liées à la cybercriminalité ont été recensées l'an passé et ces attaques visent particulièrement les hôpitaux.
En février 2021, le secrétaire d'État à la transition numérique révélait l'existence de 27 cyberattaques d'hôpitaux en 2020 et 2021 (premier trimestre).
"*Le secteur de la santé et de l'action sociale est celui pour lequel le nombre de notifications de violations de données personnelles a le plus progressé par rapport à 2019*". Il a augmenté de 83%, atteignant 319 notifications. En comparaison, la CNIL a reçu 2.825 notifications tous secteurs confondus, en hausse de 23% par rapport à 2019.

Alors que les attaques de ce type se multiplient, touchant tous les secteurs et en particulier celui de la santé, en France comme à l'international, le Président de la République a présenté le 18 février 2021 l'accélération de la **stratégie nationale en matière de cybersécurité**. Celle-ci vise à structurer l'écosystème cyber et à le rendre plus robuste pour permettre aux acteurs nationaux de se doter de moyens renforcés et souverains en matière de cybersécurité.

« Notre stratégie en matière de cybersécurité va accélérer. Car il nous faut aller plus loin, plus vite, être à l'avant-garde. Au total, 1 milliard d'euros seront investis.
Il nous faut renforcer les formations et doubler à l'horizon 2025 le nombre d'emplois dans ce secteur stratégique.
Les structures de santé seront invitées à consacrer systématiquement 5 à 10 % du budget à la cybersécurité, notamment au maintien en condition de sécurité des SI dans la durée. »

Emmanuel Macron
Président de la République Extraits de la déclaration du 18 février 2021

Après l'attaque contre les hôpitaux de Dax et de Villefranche-sur-Saône Emmanuel Macron a annoncé de nouveaux moyens pour lutter contre la cybercriminalité dans le secteur de la santé. Parmi le plan de Relance, la transition numérique a été qualifiée de priorité avec une enveloppe de 7 milliards d'euros. La santé va bénéficier d'un milliard d'euros « consacré à la remise à niveau des services publics et deux milliards dans le Ségur de la santé sur le volet numérique » a indiqué le président. Sur la somme attribuée aux Ségur 350 millions « seront dédiés à renforcer la sécurité des systèmes d'information de santé ».

Déclinaison pour les établissements hospitaliers de la stratégie nationale pour la cybersécurité, le **plan de renforcement de la sécurité** en santé lancé par le ministère de la santé s'appuie sur les déclinaisons de la feuille de route du numérique en santé et du volet numérique du Ségur.

L'appui aux structures de santé réalisé par le CERT santé (ex-cellule d'accompagnement cybersécurité des structures de santé -ACSS- de l'ANS) et la **campagne "tous cybervigilants"** complètent le dispositif national.

« Avec le Ségur de la Santé, nous avons fait le choix d'investir massivement dans la sécurité des systèmes d'information de santé. Confirmé par les récentes annonces du Président de la République, notre engagement porte en premier lieu sur la prévention en donnant aux établissements la capacité de mettre en œuvre les outils pour augmenter leur niveau de protection. Cette prévention prend également la forme d'audits de sécurité des systèmes d'information et de sessions de sensibilisation. L'autre volet de notre engagement porte la réponse proprement dite aux incidents ».

« C'est par la pédagogie, la formation, le soutien en moyen humain et financier, l'accompagnement des acteurs, que nous sécuriserons ensemble les pratiques du numérique en santé.
Alors je vous le demande, soyons TOUS CYBERVIGILANTS ! »

Olivier Véran
Ministre des Solidarités et de la Santé

2. Notre vision

La FEIMA se félicite des décisions politiques qui ont été adoptées pour lutter contre la cybercriminalité dans le secteur de la santé et des actions qui sont portées par le ministère de la santé pour renforcer la sécurité des systèmes d'informations de santé et sensibiliser l'ensemble des acteurs concernés via la campagne « Tous Cybervigilants ! ».

Elle déplore cependant que ces leviers d'actions ne soient à ce jour prioritairement ciblés que sur le secteur hospitalier, certes plus sensible aux cyberattaques, sans prendre en compte le secteur ambulatoire dont les acteurs en sont d'ores et déjà victimes. Une prise en compte d'autant plus importante que les prochaines années seront caractérisées par une transformation du système de santé reposant sur une interconnexion croissante de l'ensemble des acteurs, offrant ainsi de multiples portes d'entrées aux actes cyber malveillants.

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.

Aujourd'hui, plus que jamais, les professionnels de santé doivent pouvoir compter sur des experts au savoir-faire et à l'éthique irréprochables pour exercer dans l'environnement le plus sûr possible.

Conscients des enjeux sécuritaires et éthiques qui conditionnent la dynamique d'accélération du numérique en santé à l'œuvre, les éditeurs membres de la FEIMA font preuve d'une mobilisation de longue date pour assurer la disponibilité, l'intégrité, la confidentialité et la traçabilité de l'information médicale, dans le respect du cadre législatif et règlementaire.

Ils se sont en outre récemment impliqués dans la conception des critères « d'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.

3. L'engagement des membres de la FEIMA

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 visant à renforcer les réponses sécuritaires et éthiques à apporter au secteur ambulatoire**.

Ces dispositions se traduisent par l'élaboration d'une **charte « Engagé pour la cybersécurité »** destinée à s'appliquer à chacun des membres de la fédération et à tout nouvel acteur industriel souhaitant rejoindre ses rangs.
Une charte qui fixe les lignes de conduites à respecter pour répondre aux obligations sécuritaires et éthiques, ainsi que les actions de sensibilisation et d'accompagnement à mettre en œuvre auprès des professionnels de santé pour qu'ils prennent la pleine mesure de leur rôle de responsable de traitements et des dispositions qu'ils doivent adopter.

- **Conformité au RGPD**
- **Hébergements de données de santé certifiés et respectueux des impératifs de souveraineté européenne**
- **Conformité aux référentiels de la CNIL**
- **Conformité aux référentiels de la politique générale de sécurité des systèmes d'information en santé (PGSSIS)**
- **Echanges de données de santé via Messagerie Sécurisée de Santé**
- **Cryptage et anonymisation des données échangées entre acteurs de santé ou exportées à des fins d'études ou de recherche**
- **Collecte de données de santé dans le cadre strict règlementaire autorisé**
- **Respect des règles de portabilité dictées par les pouvoirs publics**
- **Démarche de mesure de la conformité des solutions logicielles et des services numériques via la plateforme CONVERGENCE (ANS)**
- **Démarches de mise en conformité avec les critères d'éthique des Logiciels de Gestion de Cabinet**
- **Promotion du « mémento de sécurité informatique pour les professionnels en exercice libéral » auprès des professionnels de santé**
- **Conseil et accompagnement des professionnels de santé**

(*) Ces critères d'engagement complètent les conditions d'admission des membres définies dans les nouveaux statuts de la fédération.

Un engagement que nous considérons comme important dans sa capacité à contribuer au renforcement des mesures éthiques et sécuritaires sur le secteur du premier recours, mais dont la pleine efficacité nécessiterait que des actions de soutien complémentaires soient engagées en direction des professionnels de santé.

La FEIMA appelle donc les pouvoirs publics à adopter des dispositions, comme elles ont pu l'être sur le secteur hospitalier, permettant de soutenir les actions de mise en conformité des professionnels de santé libéraux à l'égard des obligations qui sont les leurs en qualité de responsables de traitements.

4. Signataires

En signant la présente Charte, les signataires s'engagent à respecter l'ensemble des engagements décrits en matière de Cybersécurité.

Date : 25 octobre 2021

Francis MAMBRINI
Président de la FEIMA

Nom du signataire :
Nom de la société :