Service de santé des armées

LA LETTRE TRIMESTRIELLE DU SSA SUR LA CYBERSECURITE ET LES CYBERMENACES

Quatrième trimestre 2019

La Lettre trimestrielle évolue et devient plus interactive pour vous familiariser aux enjeux de cybersécurité dans vos usages numériques professionnels comme personnels

SENSIBILISATION

Comment sécuriser mes mots de passe ?

Adoptez les mesures de sécurité adaptées pour choisir vos mots de passe les gérer et les protéger. Simplifiez le dispositif en utilisant un gestionnaire de mots passe

L'actualité de la cybersécurité et des cybermenaces

Alors que les hôpitaux doivent continuellement faire face à des cyberattaques, les patients s'inquiètent de l'utilisation croissante de leurs données pour l'innovation

Le dossier du trimestre

L'intelligence artificielle, quelles sont les applications et les usages d'intérêt pour le SSA ?

Plan de la Lettre

Service de santé des armées

SENSIBILISATION : *La sécurité des mots de passe*

LA MENACE

Le mot de passe est le mécanisme d'authentification le plus répandu pour accéder à nos outils et applications numériques personnels ou professionnels. Pourtant, vos mots de passe, ces clés qui protègent votre sécurité numérique, sont particulièrement vulnérables. ***Pas moins de 2,2 milliards de mots de passe ont été compromis en 2019.***

Pour accéder à vos outils et applications protégés par mot de passe, les pirates utilisent principalement deux méthodes :

- les attaques par « force brute » qui visent à tester toutes les combinaisons possibles pour trouver votre mot de passe, soit à la main à partir d'informations trouvées sur vous par ingénierie sociale, soit plus souvent avec un logiciel utilisant des dictionnaires de mots de passe ;
- le vol de votre mot de passe, directement s'il est enregistré sur papier, dans un message ou un fichier, dans le navigateur d'un ordinateur ou sur un site insuffisamment protégé, ou par la ruse, en vous amenant à le divulguer en répondant à un message ou en le tapant sur un site de phishing.

Pour aller plus loin, **consultez la note technique de l'ANSSI relatives aux mots de passe** ou l'article "**16 formes d'attaques des mots de passe**".

Cliquez ici pour écouter Jenny, candidate de la Hack Academy, qui présente différentes techniques pour pirater un mot de passe

LES BONNES PRATIQUES

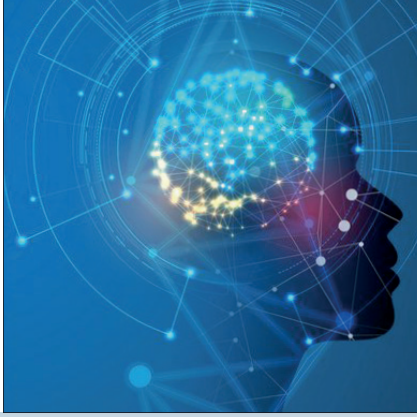
Découragez les pirates en adoptant 3 types de mesures de sécurité :

1. Choisissez vos mots de passe avec soin :

- d'une complexité suffisante si l'application ne dispose pas de mesures complémentaires comme le blocage du compte en cas d'utilisation successive d'un mot de passe erroné ou la possibilité de désactiver le compte en cas de vol du support (cas des cartes SIM ou des cartes bancaires) ;
- impossibles à deviner même par ceux qui disposent d'information sur vous ;
- différents pour chacun de vos outils et de vos comptes en ligne qui présentent un caractère sensible (banque, messagerie, réseau social, etc.).

Visitez le site de ***cybermalveillance.gouv.fr***

Service de santé des armées



SENSIBILISATION : *La sécurité des mots de passe*

PENSEZ-Y

« Deux cadenas valent mieux qu'un » (CNIL) :
Activez la double authentification lorsque votre outil numérique le propose. Cette mesure est désormais la règle au niveau de l'UE pour **les services de paiement en ligne**

COMMENT CHOISIR SON MOT DE PASSE "FORT" :

Sa longueur :

- Au moins 12 caractères en l'absence de mesures complémentaires
- 8 s'il y a des mesures de blocage

Sa complexité :

mélanger les caractères comprenant des majuscules, des minuscules, des lettres accentuées, des chiffres et des caractères spéciaux.

Vous pouvez aussi utiliser l'outil de la CNIL pour **« générer un mot de passe solide ».**

Pour comprendre la « force » d'un mot de passe, **faites le test de l'ANSSI** ou celui de **howsecureismypasseword** (sans entrer votre vrai mot de passe).

2. Gérer vos mots de passe

- Changez systématiquement les mots de passe installés par défaut sur les équipements que vous venez d'acquérir ;
- Changez toujours de mot de passe au moindre soupçon de compromission ;
- Pensez à renouveler vos mots de passe régulièrement.

3. Protéger vos mots de passe

- Ne les communiquez pas, ne les inscrivez pas sur un post-it ou sur un carnet caché dans votre tiroir, dans un fichiers texte ou un message ;
- N'enregistrez jamais un mot de passe sur un ordinateur partagé ou sur un navigateur web.

POUR RETENIR VOTRE MOT DE PASSE "FORT"

Deux méthodes conseillées par l'ANSSI :

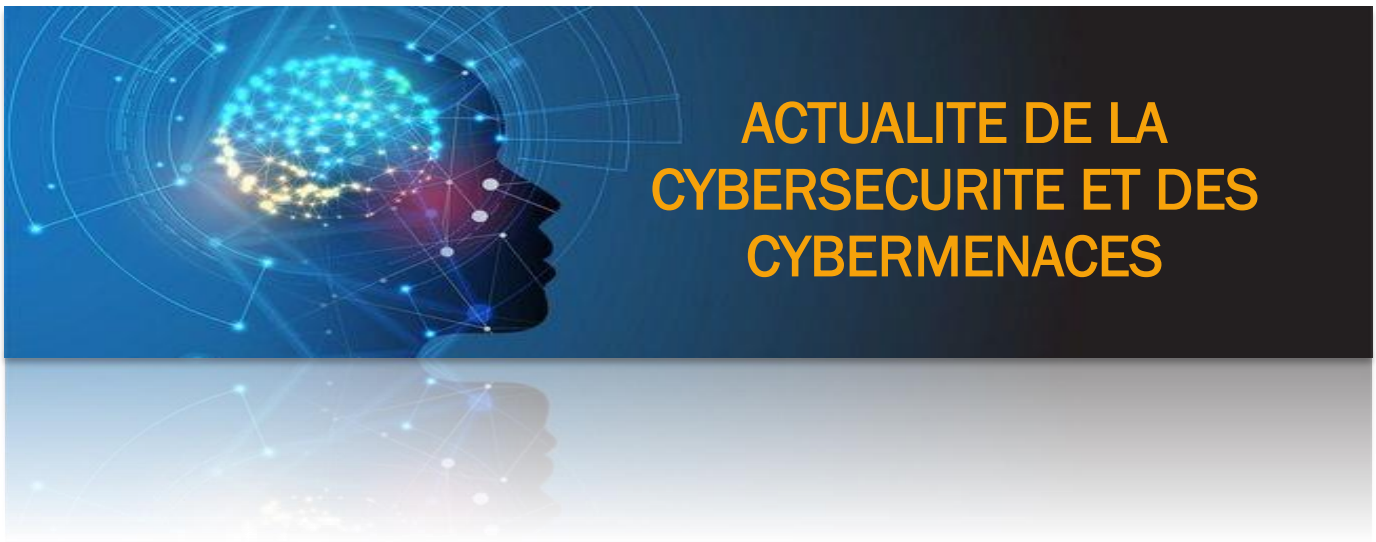
La méthode des premières lettres :
"*Un tiens vaut mieux que deux tu l'auras*" devient "*1tvmQ2tL'A*"

La méthode phonétique :
"J'ai acheté huit CD pour cent euros cet après-midi" devient "*ght8CD%E7am*"

Pour en savoir plus sur ces mesures de sécurité, consultez **les conseils de l'ANSSI** et de **la CNIL.**

Simplifiez le dispositif en utilisant un gestionnaire de mots de passe pour éviter de perdre ou de vous faire voler vos mots de passe

- Retenir chacun de vos mots de passe est un exercice humainement impossible. Recourir à un gestionnaire de mots de passe vous permet de stocker et de gérer l'ensemble de vos mots de passe de manière sécurisée avec du chiffrement. Vous n'aurez alors plus qu'à retenir un seul mot de passe « fort » pour accéder à tous vos outils et applications numériques.
- **Mis à disposition au sein du ministère des Armées, le logiciel Keepaass, certifié par l'ANSSI,** permet de sécuriser l'accès à vos outils numériques professionnels. Keepass permet également de générer, à votre place, des mots de passe complexes et aléatoires. La solution est disponible pour **Windows, Mac ou encore Linux** et peut être utilisée sur **portable**, sur **mobile** et sur un **navigateur**.
- Vous pouvez également utiliser ce gestionnaire pour vos besoins personnels ou d'autres gestionnaires gratuits recommandés par la CNIL comme **ZenyPass** ou **Password Safe**



ACTUALITE DE LA CYBERSECURITE ET DES CYBERMENACES

Les hôpitaux : des cibles toujours plus attractives pour les cybercriminels

Les hôpitaux du monde entier continuent à être touchés par de nombreuses cyberattaques, principalement des ransomwares (rançongiciels).

Le ransomware est en effet devenu l'une des principales cybermenaces, ciblant tous les secteurs d'activité y compris notamment les hôpitaux. Il consiste, après avoir pénétré le système d'information, à chiffrer les données et les serveurs, la clef de déchiffrement n'étant fournie par l'attaquant qu'après paiement d'une rançon, généralement en crypto-monnaie pour limiter sa traçabilité. La fin de l'année 2019 confirme cette tendance forte signalée lors de la Lettre précédente. Parmi les nombreuses victimes des dernières attaques de ce type, citons *l'hôpital d'Issoudun (Indre)* et *plusieurs hôpitaux australiens* en octobre, ou encore *les cinq sites du CHU de Rouen* en novembre.

A chaque fois, pendant plusieurs jours, l'établissement hospitalier s'est vu privé de tout ou partie de son système informatique, devant revenir dans le meilleur des cas au crayon, papier et téléphone pour la gestion des rendez-vous, des repas et des transports, et au pire, se trouvant privé d'accès à l'ensemble de ses applications médicales et aux dossiers des patients, situation particulièrement grave du fait de la dématérialisation croissante des procédures. Ainsi, certains d'entre eux, comme le CHU de Rouen, ont dû cesser toute consultation ou intervention autre que pour des urgences vitales.

Outre leur fort impact sur le fonctionnement des hôpitaux et donc sur la santé publique, ces attaques peuvent entrainer des dépenses importantes pour financer les investigations préalables par des experts, souvent longues, et les mesures de remise en état opérationnel du système d'information et de renforcement de sa sécurité. L'hôpital d'Issoudun, bien qu'ayant été faiblement affecté par l'attaque subie, a ainsi dépensé plus de 40 000 €.

Il faut parfois en outre payer la rançon, généralement très élevée, pour récupérer les données administratives et médicales en l'absence de sauvegardes récentes. A noter que son paiement ne garantit en rien de recevoir la clef de déchiffrement, ni même de récupérer la totalité des données. *Un hôpital de Brooklyn* n'avait toujours pas pu déchiffrer certaines données de patients plus de 3 mois après avoir payé les attaquants pour un ransomware subi en juillet 2019.

Enfin, ces attaques par ransomware peuvent avoir un impact supplémentaire très significatif sur les établissements de santé, tant en matière d'image que financièrement, si elles ont également donné lieu à la divulgation des données à caractère personnel. Rappelons que le *Règlement général de protection des données* (RGPD) de l'Union européenne prévoit des amendes administratives pouvant s'élever à 10 000 000 € en cas de manquement par des établissement publics à leurs obligations, comme par exemple une négligence dans l'application des mesures de cybersécurité nécessaires, que le montant de l'amende effective dépendra notamment de la

catégorie de données à caractère personnel concernées par la violation, et de ce point de vue, les données de santé y figurent parmi les plus sensibles, et enfin que toute personne ayant subi un dommage matériel ou moral du fait d'une violation du RGPD a le droit d'obtenir du responsable du traitement réparation du préjudice subi. Notons que dans les cas cités, les autorités ont presque toujours déclaré n'avoir trouvé aucune trace d'exfiltration de fichiers et donc de compromission de données sensibles. Cela reste cependant toujours difficile à affirmer.

Sur ces derniers points, les attaques par ransomware rejoignent celles visant à voler des données à caractère personnel, qui restent une autre menace forte. En octobre dernier, un *hôpital de l'État du Montana aux États-Unis* s'est ainsi fait voler les informations personnelles de 130 000 patients.

Dans la plupart des cas cités, le ransomware a pu atteindre son but du fait de défaut de sécurité du système ou d'un manque d'hygiène informatique du personnel, comme un clic malheureux sur un message de phishing. Et comme le souligne *le site Zataz.com dans un article sur l'attaque du CHU de Rouen*, les établissements français sont mal protégés : le Dark Web regorge de données de santé, de mails et d'identifiants de connexion appartenant à des cliniques et hôpitaux ; pas moins de 21 couples mails/mots de passe concernant le CHU de Rouen y ont été trouvés.

Facteur aggravant encore les risques actuels, *un nouveau mode d'action associé à un nouveau ransomware* est apparu ces derniers mois, consistant, en plus de chiffrer les données, à changer les mots de passe des postes et serveurs, les rendant totalement inutilisables, et potentiellement, à extraire de grandes quantités de données avec la menace de les rendre publiques en cas de non-paiement de la rançon.

De très nombreuses données médicales accessibles depuis l'Internet

En plus de celle de Zataz.com citée ci-dessus, deux études viennent de montrer la fréquente faiblesse de la sécurité des serveurs hébergeant les données de santé.

7Go de données de santé accessible sur un espace de stockage Amazon mal configuré

Aux États-Unis, une équipe de chercheurs a pu accéder à 7 Go de données hébergées sur un espace de stockage du Cloud d'Amazon, qu'un défaut de configuration rendait accessible à n'importe quel internaute, avec un droit d'accès « Full Control for Everyone ». Ces données, appartenant à la société de téléconsultation d'urgence pour les accidents du travail *MedCall Advisors*, comportaient des déclarations d'accidents du travail concernant 181 entreprises américaines, les informations à caractère personnel permettant de reconstituer l'état civil complet de près de 3 000 personnes et 715 fichiers audio de conversations entre patients et praticiens ayant réalisé une télé-expertise.

Des images médicales en libre accès sur Internet

Mi- septembre 2019, après avoir effectué une analyse de vulnérabilités de 2300 serveurs hébergeant des données médicales dans le monde, la société Greenbone Networks annonçait que 590 d'entre eux étaient mal sécurisés, voire dépourvus de toute forme de sécurité et donc totalement accessibles à tous depuis l'Internet. 24 millions de dossiers de patients et 400 millions d'images médicales de 52 pays étaient ainsi exposés, représentant une valeur excédant a priori un milliard de US dollars en cas de vente sur le Dark Web. 7 de ces serveurs étaient situés en France, avec 47 000 dossiers de patients et 5,2 millions d'images médicales.

Cette situation justifie pleinement les nouvelles dispositions prises par la France en 2018 pour

renforcer la sécurité des hébergeurs de santé (HDS), désormais tenus de détenir une *certification* délivrée par un organisme accrédité par le COFRAC (ou équivalent au niveau européen) après un audit vérifiant leur conformité à un référentiel spécifique.

Des vulnérabilités touchent des équipements de santé

A l'instar de la plupart des systèmes industriels, les équipements de santé comportent fréquemment des vulnérabilités logicielles, constituant autant de portes d'entrée pour des attaques informatiques qui peuvent affecter les équipements eux-mêmes voire, par rebond, l'ensemble du système d'information de l'établissement. Le maintien en condition de sécurité de ces équipements doit être une préoccupation permanente, tant lors de leur acquisition, avec des clauses exigeant l'existence d'une recherche permanente de vulnérabilités par le fabriquant et la diffusion des correctifs de sécurité nécessaires, que dans leur vie opérationnelle, avec une veille de l'établissement sur les vulnérabilités qui pourraient être découvertes et sur la publication de correctifs de sécurité, et la mise en place sans délai des mesures de contournement recommandées en attendant les correctifs, et de ces correctifs dès leur publication.

Il est en particulier nécessaire de veiller le site du Ministère des solidarités et de la santé *cyberveille-sante.gouv.fr* (onglets Alertes, Cyberveille et cyberveille Santé), qui fournit, pour chaque vulnérabilité dont il a connaissance, l'état de disponibilité des correctifs de sécurité et les mesures de contournement recommandés en attendant leur mise en place, ainsi qu'un lien sur le site du fabricant.

Il est également recommandé de consulter régulièrement les sites des fabricants des différents équipements détenus, forcément plus à jour que celui du ministère.

Parmi les vulnérabilités en cours, citons :

- Une *faille de sécurité dans les appareils Valleylab FT10 et FX8 de Medtronic* ;
- Une *faille de sécurité dans la solution Philips de gestion des données obstétricales IntelliSpace Perinatal.*

Une inquiétude sur l'utilisation croissante des données de santé pour l'innovation

Dans le monde, des accords se nouent de plus en plus entre des acteurs de santé et des entreprises informatiques pour développer des innovations à vocation médicale basées sur l'intelligence artificielle (IA), cristallisant des questions sociétales quant à l'utilisation des données de santé.

Ascension transmet les données de santé de millions d'Américains à Google

Le 12 novembre 2019, le *Wall Street Journal* a divulgué un accord de partenariat signé entre Google et Ascension, l'un des plus grands acteurs de la santé aux États-Unis avec 2600 sites de soins, dont 150 hôpitaux et 50 maisons de personnes âgées, s'émouvant du projet secret Nightingale de Google d'amasser les données de santé de millions d'Américains sans les en informer. Ascension fait ainsi héberger ses données sur la plate-forme Google Cloud, transférant des dossiers médicaux complets (identité des patients, diagnostics, résultats d'examens et antécédents) qui permettra à Google de développer, grâce à l'intelligence artificielle, des outils permettant de suggérer aux médecins des examens complémentaires, des prestations supplémentaires ou des traitements, voire d'identifier des anomalies dans le parcours de soins.

En Chine, un accord entre deux géants sur le développement de solutions basées sur l'intelligence artificielle

Inspur, une entreprise publique géante d'électronique et d'informatique, et Baidu, célèbre pour son moteur

de recherche, le 3ème site le plus consulté au monde, viennent de signer un accord de coopération stratégique prévoyant notamment de construire ensemble de nombreuses applications et des services basés sur l'IA dans le domaine de la santé, comme des systèmes d'aide à la décision clinique, de dépistage intelligent du fond d'œil ou d'assistance au diagnostic. L'origine des données de santé n'est pas dévoilée, mais il est probable qu'elles proviendront en autres du Cloud d'Inspur et des immenses bases de données de Baidu, à l'insu de la population.

En France, les CHU pointent un besoin de confiance dans la mise en place des entrepôts de données de santé

Les professionnels de santé craignent un blocage d'ordre culturel, comme la peur des patients et des soignants que leurs données soient utilisées à des fins de surveillance par exemple, dans la constitution des *entrepôts de données de santé* (EDS), ces outils informatiques permettant la collection, l'intégration puis le traitement des données de santé provenant d'un grand nombre de sources d'information clinique (dossier patient informatisé, système d'information des laboratoires et d'imagerie, prescription informatisée, dossier infirmier …). Il convient de rappeler que la mise en œuvre des EDS est strictement encadrée par le RGPD et les dispositions nationales complémentaires de la loi Informatique et liberté, et nécessite une autorisation explicite de la CNIL.

Les mesures de cybersécurité et de lutte contre les cybermenaces dans la santé

L'ASIP Santé précise des mesures de sécurité nécessaires dans le déploiement de la télémédecine

Dans un rapport récent sur l'accompagnement du déploiement de la télémédecine, l'ASIP Santé a précisé un certain nombre de mesures de sécurité nécessaires, parmi lesquelles l'authentification des acteurs et des exigences minimales de sécurité à imposer aux éditeurs de solutions techniques, et a présenté une étude sur la sécurité de la vidéotransmission dans le cadre de la téléconsultation.

L'authentification multi-facteurs bloque 99,9% des cyberattaques automatisées

Dans un contexte de cyberattaques de plus en plus fréquentes et importantes, le site américain *HIPAA Journal* rappelle la fragilité des authentifications par login - mot de passe, du fait des mauvaises pratiques des usagers pour le choix et la gestion de leur mot de passe et des fréquentes fuites des mots de passe par phishing ou par attaque de sites mal protégés. En conséquence, il recommande l'usage de l'authentification multi-facteurs, qui permet de bloquer 99,9% des attaques automatisées. L'authentification multi-facteurs consiste à utiliser plus d'une méthode pour vérifier l'identité de l'usager, comme l'utilisation d'une carte à puce, d'une authentification biométrique ou d'un SMS transmis par téléphone, venant compléter, par exemple, le login - mot de passe classique.

L'INTELLIGENCE ARTIFICIELLE, QUELLES SONT LES APPLICATIONS ET USAGES D'INTERET POUR LE SSA ?

L'Intelligence artificielle (IA) en santé est un marché en plein essor, tiré par des très nombreuses recherches et innovations. Selon le rapport final de l'étude Pipame « *Intelligence artificielle – État de l'art et perspectives pour la France* », « *le marché mondial de l'intelligence artificielle dans le secteur de la santé {…} pourrait atteindre 6,6 Mds de dollars en 2021, contre 634 M$ en 2014* ».

Née dans les années 1950, l'IA est une notion mouvante difficile à définir. Elle consiste à doter des machines de la capacité « de simuler l'intelligence et d'accomplir automatiquement des tâches de perception, de compréhension et de prise de décision ». Concrètement, l'IA repose sur des traitements de données qui utilisent des algorithmes reproduisant l'activité du cerveau humain. Aujourd'hui, elle utilise déjà des algorithmes variés permettant par exemple le traitement des images et du langage ou encore l'apprentissage automatique. Si l'IA offre dès à présent des opportunités indéniables pour le secteur de la santé, avec un certain nombre d'applications matures, elle reste encore en pratique un domaine en plein développement. Comme le souligne l'Inserm, « *le robot omniscient, qui pour beaucoup symbolise l'IA, n'est pas pour demain !* ». Par ailleurs, le développement de l'IA pose un certain nombre de questions de nature éthique, juridique et de sécurité.

Usages et opportunités de l'IA dans le secteur de la santé

Le rapport final de l'étude Pipame précédemment mentionnée a identifié 4 grands domaines d'usages de l'IA dans le secteur de la santé et, au sein de ces domaines, des usages aujourd'hui matures.

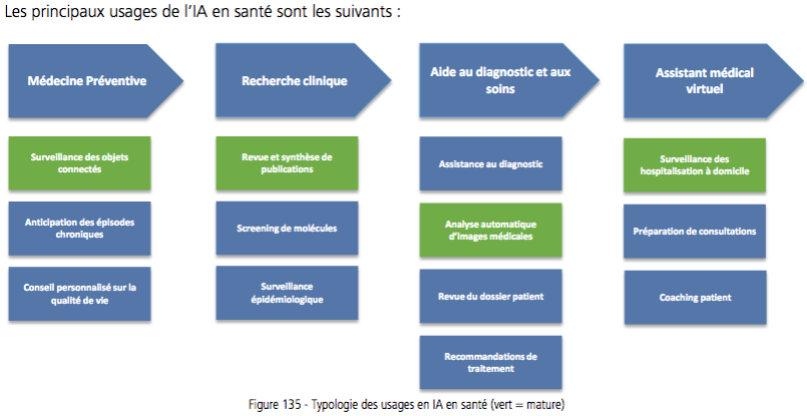


Figure 135 - Typologie des usages en IA en santé (vert = mature)

(*Source :* https://www.entreprises.gouv.fr/files/files/directions_services/etudes-et-statistiques/prospective/Intelligence_artificielle/2019-02-intelligence-artificielle-etat-de-l-art-et-perspectives.pdf)

- **La médecine préventive** : l'IA offre la possibilité de prévenir l'apparition d'une maladie chez un patient ou son évolution en anticipant des épisodes chroniques ou en permettant au patient d'améliorer sa qualité de vie. Avec le développement des objets connectés de santé, l'IA est désormais utilisée pour optimiser et accélérer l'analyse des données collectées par les capteurs médicaux, par exemple pour prévenir un risque d'insuffisance cardiaque avec un *électrocardiographe connecté*. Cet usage de l'IA peut être notamment utile pour le SSA pour évaluer la forme physiologique des soldats en entrainement ou en opération. A titre d'exemple, *BE.CARE*, une société Suisse, propose des applications de l'IA avec des objets connectés pour « *mesurer et classifier la fatigue* » ou pour *évaluer et améliorer la pratique sportive*. Le *département de la défense américaine* (DOD) utilise également l'IA pour prévenir les risques de blessures ou de maladies des soldats, notamment avec le dispositif *The Medical Readiness Tool (MRAT)*.

Écosystème inCORPUS de BE.CARE

(Source : https://www.becare.swiss/wp-content/uploads/2019/01/be.care-SA-Dossier-de-presse-FR.pdf)

- **La recherche clinique** : les centres d'étude et les laboratoires pharmaceutiques ont de plus en plus recours à l'IA pour croiser et analyser plus rapidement les données issues de la recherche. Les capacités de l'IA sont notamment utilisées en épidémiologie et pourraient contribuer à l'amélioration des politiques de santé ou encore à mieux détecter des épidémies par exemple. En matière de recherche, l'IA est surtout utilisée pour analyser les publications scientifiques et pour identifier de nouveaux axes de recherche. A titre d'exemple, la *société française Owkin* s'est associée avec *l'Inserm* et *l'AP-HP* pour développer des algorithmes qui interprètent les bases de données biomédicales et le profil des patients dans le but de découvrir de nouveaux traitements.

- **L'aide au diagnostic et aux soins** : l'IA devrait *révolutionner la médecine opérationnelle*, notamment avec *l'automatisation des diagnostics*, « la virtualisation et simulation des environnements opératoires » ou encore la robotisation de la prise en charge des soins. En outre, l'analyse des données du patient pourrait permettre de recommander des traitements plus personnalisés et efficaces. Dans le domaine de l'aide au diagnostic et aux soins, il existe déjà de nombreuses applications de l'IA en imagerie médicale qui sont *très performantes*, par exemple pour détecter des tumeurs cancéreuses. Des sociétés comme *CARDIOLOGS* ou *ULTROMICS* commercialisent également des applications de l'IA pour diagnostiquer des arythmies cardiaques à partir d'images d'électrocardiogrammes.

(Source : https://www.ultromics.com/platform/)

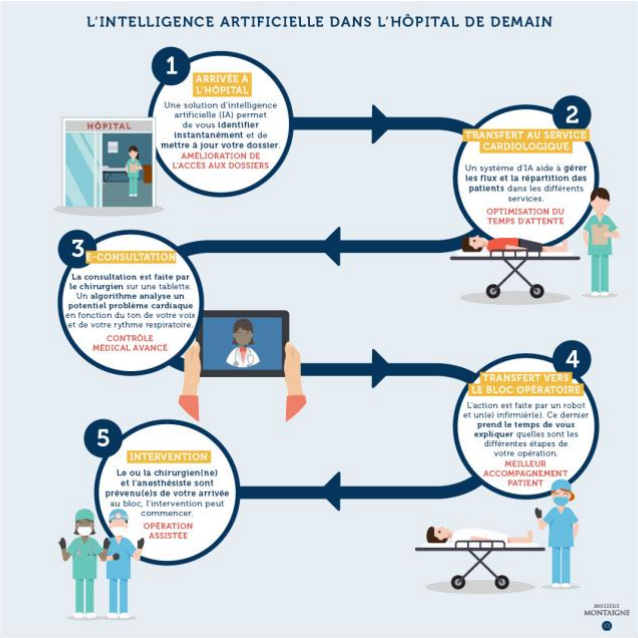
Pour la première fois, *l'Agence américaine du médicament (FDA)* a autorisé en 2018 la commercialisation de *l'application d'IA IDx-DR* de diagnostic sans médecin des risques de rétinopathie diabétique grâce l'analyse d'images rétiniennes.

Source : https://www.eyediagnosis.co/idx-dr-eu-1

- **L'assistant médical virtuel** : dans le cadre de cet usage, l'IA devrait *bouleverser la relation médecins-patients* et notamment *renforcer l'autonomie du patient*. Aujourd'hui, les médecins et les patients peuvent être assistés administrativement ou médicalement par des applications d'IA. Par exemple, en utilisant les techniques de traitement automatique du langage et d'apprentissage, certaines applications comme *BABYLON HEALTH* proposent un *agent conversationnel* pour interroger le patient sur ses symptômes et le conseiller ou pour lui proposer une consultation avec un médecin (pour comprendre comment l'application fonctionne, *visualiser la vidéo youtube*).

L'IA est désormais présent dans la plupart des domaines de la santé et ses différentes applications devraient être utilisées dans l'ensemble du parcours de soin du patient, de sa prise en charge administrative et médicale à sa remédiation.

Exemple des opportunités de l'IA dans un parcours de soin hospitalier



(*Source : https://www.institutmontaigne.org/publications/ia-et-emploi-en-sante-quoi-de-neuf-docteur*)

Limites et risques de l'IA

L'essor de l'IA dans la santé pose de nombreuses questions qui freinent son développement et qui soulèvent un certain nombre de risques pour les professionnels de santé, les patients ou encore la santé publique.

- ***L'accès aux données de santé*** : le développement de *l'IA nécessite d'utiliser de très nombreuses données* pour obtenir des résultats satisfaisants. Or, la législation en vigueur sur la protection des données à caractère personnel *rend difficiles l'accès aux données de santé et leur utilisation*.
  A ce titre, le « *Rapport de Cédric Villani : donner un sens à l'intelligence artificielle* » préconise d'assouplir la législation en vigueur dans le cadre d'expérimentations. Dans cet esprit, le ministère de la santé a mis en place

un « *Health Data Hub* », une plateforme d'exploitation des données de santé, qui permettra d'alimenter en données, de manière responsable, les applications d'IA expérimentées par les professionnels de santé.

- ***L'éthique et la responsabilité juridique dans le recours à l'IA*** : les capacités de l'IA à orienter les décisions et la complexité des algorithmes voire leur opacité peuvent entrainer des risques de discrimination, d'exclusion ou encore d'erreur pouvant entrainer une faute médicale par exemple.
  Un *cadre juridique dédié à l'IA est en construction* afin notamment de lutter contre les biais algorithmiques. Dans son rapport, Cédric Villani a également souligné que l'IA ne devait pas remplacer le médecin et demeurer un outil d'aide à la décision.

- ***Des risques en matière de cybersécurité*** : le recours l'IA en santé nécessite de mettre en œuvre de grandes bases de données de santé qui pourraient devenir des cibles privilégiées des pirates informatiques entrainant alors des risques de fuites de données massives. Par ailleurs, les algorithmes d'IA peuvent faire l'objet de détournements à des fins malveillantes.

- ***Un risque « d'ubérisation » de la santé*** : les entreprises du numérique comme les GAFAM développent des services de santé personnalisés grand public grâce à l'IA et pourraient ainsi entrer en concurrence avec les professionnels de santé, ce qui pourrait entrainer deux risques :
  - un *risque d'utilisation des données de santé des patients à des fins de profilage commercial* ;
  - un risque d'exercice « sauvage » de la médecine potentiellement préjudiciable pour la santé publique.

Conclusion

Si les problématiques de l'IA et ses usages en santé sont encore en voie de développement, les applications d'IA tendent à se multiplier rapidement, notamment avec le déploiement des objets connectés qui permettent de recueillir de nombreuses données sur les maladies et les patients. La combinaison des algorithmes d'IA (apprentissage, traitement automatique du langage ou des images par exemple) et des objets connectés devrait d'ailleurs renforcer les usages de l'IA dans la médecine opérationnelle avec le développement d'applications dédiées à l'aide au diagnostic et aux soins ou encore à l'assistance des médecins ou des patients en temps réel. Notons d'ailleurs que le remboursement des dispositifs médicaux utilisant l'IA fait actuellement l'objet d'une évaluation de la Haute Autorité de Santé (HAS) qui vient de lancer *une consultation publique sur le sujet*.

BIBLIOGRAPHIE

- **Sensibilisation**

https://www.tech2tech.fr/collection-1-a-5-le-plus-gros-dump-de-mots-de-passe-de-lhistoire/

https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_MDP_NoteTech.pdf

https://assiste.com/Mots_de_passe_Formes_d_attaques.html

https://www.hack-academy.fr/candidats/jenny

https://www.cybermalveillance.gouv.fr/nos-articles/video-gerer-ses-mots-de-passe/

https://www.cnil.fr/fr/generer-un-mot-de-passe-solide

https://www.ssi.gouv.fr/administration/precautions-elementaires/calculer-la-force-dun-mot-de-passe/

https://howsecureismypassword.net/

https://www.defense.gouv.fr/fre/terre/actu-terre/cyber-l-armee-de-terre-innove-pour-repondre-aux-menaces

https://keepass.info/

https://keepass.fr/

https://keepass.fr/telecharger-et-utiliser-keepass-portable/

https://keepass.fr/keepass-pour-mobile-android-et-ios/

https://keepass.fr/keepass-pour-navigateur-chrome-firefox-et-safari/

https://zenyway.com/password-manager/home/en/index.html

https://pwsafe.org/

https://www.cybermalveillance.gouv.fr/wp-content/uploads/2019/06/mots-de-passe.pdf

https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires

https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32015L2366

- **Actualité**

https://www.lequotidiendumedecin.fr/hopital/exercice/ranconne-par-des-pirates-lhopital-dissoudun-en-etat-de-crise-pendant-48-heures

https://www.theguardian.com/australia-news/2019/oct/01/systems-shut-down-in-victorian-hospitals-after-suspected-cyber-attack

http://www.leparisien.fr/economie/frappe-par-une-cyberattaque-le-chu-de-rouen-a-tourne-au-ralenti-ce-week-end-17-11-2019-8195340.php

https://www.hcinnovationgroup.com/cybersecurity/data-breaches/news/21113557/ransomware-attack-hits-brooklyn-hospital-center-some-patient-data-unrecoverable

https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:02016R0679-20160504

https://nbcmontana.com/news/local/cyberattack-on-montana-medical-clinic-breaches-patient-data

https://www.zataz.com/chantage-numerique-a-lencontre-du-chu-de-rouen/

https://www.01net.com/actualites/megacortex-le-ransomware-qui-menace-de-publier-vos-donnees-en-plus-de-les-chiffrer-1800757.html

https://www.dsih.fr/article/3061/un-espace-de-stockage-amazon-mal-configure-et-des-donnees-de-sante-une-nouvelle-fois-exposees.html

https://medcalladvisors.com/

https://www.greenbone.net/wp-content/uploads/Confidential-patient-data-freely-accessible-on-the-internet.pdf

https://esante.gouv.fr/labels-certifications/hebergement-des-donnees-de-sante

https://cyberveille-sante.gouv.fr/

https://www.cyberveille-sante.gouv.fr/cyberveille-sante/1496-decouverte-de-vulnerabilites-critiques-dans-les-appareils-valleylab-ft10-and

https://www.cyberveille-sante.gouv.fr/cyberveille-sante/1480-decouverte-dune-vulnerabilite-dans-la-solution-philips-de-gestion-des

https://www.lemonde.fr/economie/article/2019/11/12/l-accord-controverse-de-google-avec-plus-de-cent-cinquante-hopitaux-aux-etats-unis_6018878_3234.html

https://www.wsj.com/articles/google-s-secret-project-nightingale-gathers-personal-health-data-on-millions-of-americans-11573496790?mod=hp_lead_pos1

https://www.jqknews.com/news/310272-Baidu_and_Inspur_have_reached_strategic_cooperation_to_promote_the_rapid_implementation_of_AI_in_medical_and_other_fields.html

https://www.ticsante.com/story/4831/entrepots-de-donnees-de-sante-les-chu-pointent-un-besoin-de-confiance-et-de-competences.html

http://www.chu-rouen.fr/cismef/wp/wp-content/uploads/2019/01/EDS-Rouen-janvier-2019-pour-GSM3.pdf

https://esante.gouv.fr/sites/default/files/media_entity/documents/asip_etude_telemedecine_synthese_v0.45.pdf

https://www.hipaajournal.com/multi-factor-authentication-blocks-99-9-of-automated-cyberattacks/

- **Dossier**

https://www.entreprises.gouv.fr/files/files/directions_services/etudes-et-statistiques/prospective/Intelligence_artificielle/2019-02-intelligence-artificielle-etat-de-l-art-et-perspectives.pdf

https://www.inserm.fr/information-en-sante/dossiers-information/intelligence-artificielle-et-sante

https://comparatif-logiciels-medicaux.fr/test-de-myecg-de-bewell-connect-mini-ecg-pour-patients-arythmiques

https://www.becare.swiss/fr/savoir-faire/

https://actu.epfl.ch/news/une-application-pour-mesurer-et-classifier-la-fa-4/

https://www.becare.swiss/wp-content/uploads/2019/01/be.care-SA-Dossier-de-presse-FR.pdf

https://www.cnas.org/publications/commentary/predictive-medicine-where-the-pentagon-and-silicon-valley-could-build-a-bridge-in-artificial-intelligence

https://www.army.mil/article/159086/medical_readiness_assessment_tool_mrat

https://owkin.com/

https://www.decision-sante.com/actualites/breve/2018/04/05/insermowkin-un-partenariat-fondamental-pour-la-recherche-medicale_27383

https://www.mypharma-editions.com/lap-hp-et-owkin-sassocient-pour-accelerer-la-recherche-clinique-grace-a-lintelligence-artificielle

https://santeos.com/content/dam/santeos/documents/position-paper-medecine-augmentee-l-intelligence-artificielle-revolutionne-la-pratique-medicale-par-santeos-et-sorbonne-universite.pdf

http://fondationrechercheaphp.fr/promesses-de-lintelligence-artificielle-sante/

https://www.lemonde.fr/sciences/article/2019/05/07/comment-l-intelligence-artificielle-va-bouleverser-les-professions-de-sante_5459387_1650684.html

https://cardiologs.com/

https://www.ultromics.com/

https://www.fda.gov/news-events/press-announcements/fda-permits-marketing-artificial-intelligence-based-device-detect-certain-diabetes-related-eye

https://www.eyediagnosis.co/

https://www.eyediagnosis.co/idx-dr-eu-1

https://www.ultromics.com/platform/

https://www.conseil-national.medecin.fr/sites/default/files/external-package/edition/od6gnt/cnomdata_algorithmes_ia_0.pdf

https://www.institutmontaigne.org/blog/lia-en-sante-un-outil-au-service-des-medecins-mais-aussi-des-patients

https://www.babylonhealth.com/product

https://business.lesechos.fr/entrepreneurs/actu/0601742910225-babylon-health-la-start-up-montante-de-la-telemedecine-331379.php

https://www.youtube.com/watch?v=nm5PKFLGre0

https://www.institutmontaigne.org/publications/ia-et-emploi-en-sante-quoi-de-neuf-docteur

https://www.cnil.fr/fr/sante

https://www.sciencesetavenir.fr/high-tech/intelligence-artificielle/l-intelligence-artificielle-ferait-au-mieux-aussi-bien-que-les-medecins_137585

http://www.ticpharma.com/story/873/l-essor-de-l-ia-en-sante-freine-par-la-difficulte-d-acces-aux-donnees.html

https://www.enseignementsup-recherche.gouv.fr/cid128577/rapport-de-cedric-villani-donner-un-sens-a-l-intelligence-artificielle-ia.html

https://drees.solidarites-sante.gouv.fr/etudes-et-statistiques/acces-aux-donnees-de-sante/article/health-data-hub

https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf

https://www.usine-digitale.fr/article/l-unesco-a-18-mois-pour-elaborer-un-cadre-normatif-autour-de-l-intelligence-artificielle.N906344

https://www.nytimes.com/2019/03/21/science/health-medicine-artificial-intelligence.html

https://www.atlantico.fr/decryptage/3582741/ce-que-nous-reserve-l-offensive-des-gafam-sur-le-secteur-de-la-sante-nightingale-fitbit-donnees-personnelles-hopitaux-google-wall-street-journal-david-fayon-

https://theconversation.com/medecine-personnalisee-attention-a-la-collecte-massive-des-donnees-124520

https://www.hospitalia.fr/Evaluation-des-dispositifs-medicaux-avec-intelligence-artificielle-la-HAS-lance-une-consultation-publique_a1993.html

Plan de la Lettre

SENSIBILISATION 2

ACTUALITE DE LA CYBERSECURITE ET DES CYBERMENACES 4

LES HOPITAUX : DES CIBLES TOUJOURS PLUS ATTRACTIVES POUR LES CYBERCRIMINELS 4
DE TRES NOMBREUSES DONNEES MEDICALES ACCESSIBLES DEPUIS L'INTERNET 5
DES VULNERABILITES TOUCHENT DES EQUIPEMENTS DE SANTE 6
UNE INQUIETUDE SUR L'UTILISATION CROISSANTE DES DONNEES DE SANTE POUR L'INNOVATION 6
LES MESURES DE CYBERSECURITE ET DE LUTTE CONTRE LES CYBERMENACES DANS LA SANTE 7

L'INTELLIGENCE ARTIFICIELLE, QUELLES SONT LES APPLICATIONS ET USAGES D'INTERET POUR LE SSA ? ... 8

USAGES ET OPPORTUNITES DE L'IA DANS LE SECTEUR DE LA SANTE 8
LIMITES ET RISQUES DE L'IA 10
CONCLUSION 11

BIBLIOGRAPHIE 12

Cette Lettre trimestrielle est réalisée pour la DCSSA par CEIS