LE GUIDE DE LA CYBERSÉCURITÉ

pour les médecins libéraux

Synchronizing Healthcare

CGM CompuGroup Medical

SOMMAIRE

01

La cybersécurité, c'est quoi ?

?

"Je ne comprends pas bien en quoi c'est si dangereux d'envoyer depuis ma messagerie personnelle une information médicale sur un patient à un collègue spécialiste pour avoir son avis. C'est une question de praticité et de rapidité d'échange au service de la continuité des soins. J'utilise un mot de passe et il me semble que c'est un canal sécurisé qui respecte la confidentialité des données."

Dominique, Médecin généraliste.

Notre point de vue d'expert

"C'est une question fréquente et légitime pour tous les professionnels de santé libéraux. Les messageries personnelles sont généralement bien moins sécurisées que les messageries spécialisées. On vous en dit plus sur les enjeux de la cybersécurité dès la page suivante..."

LES ENJEUX DE LA CYBERSÉCURITÉ

Les pratiques médicales évoluent avec les technologies de l'information et de la communication pour optimiser la prise en charge des patients d'une part et améliorer l'exercice médical d'autre part. Ces évolutions de pratique nécessitent une prise de précaution de sécurité importante à titre préventif pour assurer la disponibilité, l'intégrité, la confidentialité et la traçabilité de l'information médicale. Ces quatre points fondamentaux constituent les enjeux majeurs de la cybersécurité.

1 LA DISPONIBILITÉ

La disponibilité du Sytème d'Information (SI), ou plus simplement du logiciel métier, garantit un accès permanent aux données des patients. Une atteinte à la disponibilité des données de santé peut engendrer des retards importants dans la prise en charge du patient : report de consultation vitale, erreur de soins, mauvaise posologie, double vaccination, intolérance médicamenteuse...

2 L'INTÉGRITÉ

L'intégrité des données de santé est le gage de la fiabilité et l'exactitude des données c'est-à-dire leur validité, leur cohérence et leur exhaustivité. Un défaut d'intégrité des données de santé peut entrainer une perte d'information importante sur l'état de santé d'un patient et provoquer des erreurs médicales.

3 LA CONFIDENTIALITÉ

La confidentialité des données permet de réserver l'accès aux données aux cercles de personnes autorisées. Une perte de confidentialité des données du patient peut lui porter préjudice et l'exposer à un vol de données ou à une utilisation de ces informations de santé sans son accord au profit d'un tiers (assurance, employeur, entreprise à but lucratif...). La perte des données implique également le professionnel de santé, responsable du traitement des données, qui risque des amendes très lourdes et une atteinte à sa réputation.

4 LA TRAÇABILITÉ

La traçabilité est importante en cas de dysfonctionnement pour en déterminer l'origine. Un manque de traçabilité correspond à un défaut de preuve qui peut exposer à des erreurs médicales et engager la responsabilité du médecin.

SIGNIFICATIONS ET TERMINOLOGIES : COMPRENDRE LA CYBERSÉCURITÉ

Le jargon informatique pouvant être aussi complexe qu'une encyclopédie médicale, il est important de définir quelques mots clés que vous retrouverez au fil de la lecture de ce guide.

La cybersécurité

La cybersécurité représente l'ensemble des moyens et techniques mis en oeuvre par une organisation pour assurer la sécurité du système d'information et des données informatiques. Elle porte aussi bien sur la protection des données que sur l'attaque des équipements informatiques. Selon l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), la cybersécurité est « l'état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données ».

La cybercriminalité

La cybercriminalité correspond à l'ensemble des actes illégaux de la part d'individus ou organisations, utilisant les réseaux ou les systèmes d'information, pour commettre des délits ou des crimes.

Les données personnelles

Les données personnelles sont définies par le CNIL (Commission Nationale de l'Informatique et des Libertés) comme étant des informations se rapportant à des personnes physiques identifiées ou identifiables soit directement avec leur nom et prénom soit indirectement avec un numéro d'identifiant, de téléphone ou des données biométriques. Ces données doivent être protégées en prenant des mesures adéquates.

Le traitement des données personnelles

Le traitement de données personnelles est une notion très large qui, selon la CNIL, correspond aux opérations portant sur les données personnelles à différentes étapes de leur traitement telles que « la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation, la modification, l'extraction, la consultation, l'utilisation, la communication par transmission diffusion ou toute autre forme de mise à disposition ».

LA CYBERSÉCURITÉ, UNE DISCIPLINE EN PLEINE MUTATION

La cybersécurité entre dans une démarche d'amélioration continue qui évolue au cours du temps en fonction du contexte règlementaire et environnemental. La France, comme d'autres pays, vient de vivre une crise sanitaire sans précédent avec la Covid-19, provoquant une augmentation significative des usages numériques. La télémedecine a ainsi vécu une croissance exponentielle, entraînant malheureusement avec elle une croissance tout aussi impressionnante des actes malveillants sur les données de santé.

L'environnement

La pandémie du Covid-19 est un exemple édifiant de la nécessité d'une démarche de cybersécurité constante. En effet, les organisations malveillantes ont pu profiter du manque de vigilance des personnes utilisant l'informatique. La santé étant l'un des secteurs les plus vulnérables sur le plan de la cybersécurité, l'Organisation Mondiale de la Santé (OMS) a tiré la sonnette d'alarme en publiant des mises en garde contre les fraudeurs qui essayent de se faire passer pour elle. Depuis le début de la pandémie, on déplore une hausse de cyberattaques qui seraient multipliées par cinq, et qui visent à la fois les professionnels de santé et les citoyens.

La règlementation

Le RGPD (Règlement Général sur la Protection des Données) encadre le traitement des données personnelles sur l'ensemble du territoire européen depuis le 25 mai 2018, afin de répondre aux évolutions importantes des technologies et des usages du numérique ces dernières années. En France, ce règlement s'inscrit dans la continuité de la loi informatique et liberté du 6 Janvier 1978 qui régit la liberté de traitement des données personnelles. Le RGPD s'applique à toute organisation grande ou petite, publique ou privée, qui traite des données personnelles.

LA CYBERCRIMINALITÉ, L'ÉTAT DES LIEUX

LA CYBERCRIMINALITÉ EN QUELQUES CHIFFRES

978
millions de personnes concernées par une cyberattaque chaque année dans le monde

+ 200 %
de cyberattaques en France en avril 2020

300 000
ordinateurs infectés dans 16 centres de santé britanniques en mai 2017. Le système de santé britannique (NHS) est visé par une attaque via ransomware.

121
incidents signalés à l'ANS au seul mois de mai 2020 contre 392 pour toute l'année 2019

600
ordinateurs du CHU de Montpellier sont infectés à cause d'un clic sur un courriel d'hameçonnage par un salarié en mars 2019

+ 600 %
de phishing en Mars 2020 selon l'APSSIS

LES ATTAQUES ET ARNAQUES LES PLUS COURANTES

- **L'hameçonnage ou le phishing** est une technique de fraude destinée à usurper l'identité d'un internaute en volant des renseignements personnels. Pendant la pandémie, l'Association Pour la Sécurité des Systèmes d'Information de Santé (APSSIS) a recensé plusieurs attaques par phishing sur des messageries électroniques.

- **Le harponnage** est une technique qui utilise les courriels pour mener des attaques ciblées. L'APSSIS a relevé de nombreuses diffusions de **logiciels malveillants** par courriel ayant pour objet la covid-19. Par exemple, de nombreuses personnes ont reçu des spams usurpant l'identité de l'OMS et contenant des liens ou des pièces jointes pour exécuter des **malwares** ou logiciels malveillants. D'ailleurs, des attaques aux **rançongiciels** dans le domaine de la santé sont de plus en plus fréquentes et la médecine libérale n'est pas épargnée.

- **Les arnaques** sont également de plus en plus courantes. Dernièrement, l'APSSIS a observé une arnaque au faux support technique. Il s'agissait de campagnes de pourriels incitant les utilisateurs à recourir au service support de Microsoft en cliquant sur un message frauduleux. D'autres arnaques aux FOVI (Faux ordre de virements bancaires internationaux) ont également été observés dans les établissements de santé.

- **Les vols de données personnelles** : les données patients font aussi de plus en plus l'objet de vol.

En novembre dernier le CHU de ROUEN a été victime d'une cyberattaque ! Les attaques auprès des professionnels de santé se multiplient et même l es établissements avec une DSI (Direction des Systèmes d'Information) sont victimes. Nous sommes tous concernés par la cybersécurité !

Soyons tous cybervigilants en santé !

02

La protection des données, quels enjeux pour la médecine libérale ?

"Mes logiciels médicaux sont installés sur mon ordinateur portable personnel. Cela a toujours été le cas et je me demande si je suis en tort vis-à-vis de la protection de données de mes patients. Je ne sais pas si cela est vraiment utile d'avoir un ordinateur à des fins uniquement professionnelles."

Camille, psychiatre libérale.

Notre point de vue d'expert

"Oui c'est utile. Il est important de bien séparer les environnements informatiques personnels et professionnels afin de limiter au maximum les accès aux données professionnellles. Vincent Trely apporte des éléments explicatifs page 17."

LES ENJEUX DE LA PROTECTION DES DONNÉES

LE RGPD ET LA MÉDECINE LIBÉRALE

Au sein de votre cabinet médical ou structure de santé, vous traitez et collectez des informations patients. Vous êtes donc soumis au Règlement Général de la Protection des Données (RGPD) comme toute organisation privée ou publique qui traite ou collecte des données. Il s'agit des données patients numériques via votre logiciel de gestion médical mais aussi de vos dossiers médicaux papiers. Vous devez en cas de contrôle de la CNIL être en mesure d'apporter la preuve de la mise en conformité de votre cabinet ou structure de santé.

Ce qu'il faut retenir pour votre exercice médical

1 Les informations que vous avez le droit de collecter sur votre patientèle doivent être pertinentes et limitées strictement à sa prise en charge : numéro de sécurité social, identité et coordonnées du patient, données de santé, identifiant national de santé, informations sur la situation familiale et professionnelle.

2 Vous devez définir la finalité pour chaque donnée, par exemple : la tenue du dossier médical, l'établissement et la télétransmission des documents à destination de l'assurance maladie, la télémédecine, ou encore la prise de rendez-vous.

3 Le partage des données de santé de vos patients doit être limité et les professionnels autorisés doivent pouvoir accéder uniquement aux données utiles à l'exercice de leurs missions. Par exemple, votre collègue secrétaire médicale ne pourra accéder qu'à la partie administrative du dossier patient.

4 Conformément aux recommandations du CNOM (Conseil National de l'Ordre des Médecins), les dossiers médicaux peuvent être conservés vingt ans à compter de la dernière consultation. Dans le cas où les patients décèdent dans les dix ans suivant leur dernière consultation, les dossiers doivent être conservés durant dix ans. La conservation des données de vos patients doit donc être limitée.

5 Le RGPD implique un devoir d'information auprès des personnes concernées par le traitement et la collecte de leurs données. Il s'agit d'une obligation afin de permettre à chaque patient de maitriser les données qui le concernent. Cela peut être sous forme d'affiche au sein de votre cabinet comme le propose la CNIL à titre d'exemple.

6 En tant que médecin libéral vous êtes responsable de la mise en place des mesures de sécurité garantissant la confidentialité et l'intégrité des données de santé de votre patientèle. Par exemple, sécuriser l'utilisation de votre CPS (elle est strictement personnelle) ou bien encore utiliser un mot de passe à forte authentification pour votre messagerie professionnelle.

Quels sont les risques pour les professionnels de santé ?
Le Docteur Lucas vous en parle en vidéo !

LES ATTITUDES PROFESSIONNELLES À RISQUE

VRAI OU FAUX ?

1 Dr Bourgogne reçoit Mme Picardie en consultation. Elle lui partage son désir de grossesse et lui donne des informations médicales sur sa soeur ainée qui aurait fait 2 fausses couches il y a 8 ans. **Il a le droit de noter les informations données par sa patiente dans son dossier médical informatisé.**

2 Dr Limousin, partage le même ordinateur que sa secrétaire médicale pour gagner du temps. **Ils peuvent utiliser la même session puisqu'ils sont tous les deux soumis au secret médical.**

3 Dr Aisne, cardiologue, n'a pas de secrétaire médicale et gère toute la partie administrative de son cabinet. Son antivirus est périmé depuis une semaine. **Il a raison de penser que c'est très important et voudrait s'en occuper au plus tôt.**

4 Le Dr Cher vient d'être victime d'un vol dans son cabinet. Son ordinateur a été volé. Il est rassuré car **son assurance professionnelle prendra forcément en charge le préjudice y compris celui lié à la perte des données.**

5 Dr Tarn et les infirmières libérales de la maison de santé des Coquelicots échangent souvent des messages contenant des photos de plaies sur WhatsApp afin de suivre l'amélioration des escarres de M. Occitanie. **Ils le faisaient déjà avant le confinement du mois de Mars 2020 et continuent de le faire car maintenant c'est autorisé.**

Réponses :

1. Faux. Les informations relatives à sa sœur vont au-delà des informations nécessaires au suivi de la patiente.

2. Faux. Pensez à restreindre les accès aux personnes habilitées et à sécuriser les accès aux postes par des mots de passe à authentification forte.

3. Vrai. N'oubliez pas de protéger les serveurs avec des antivirus, pare-feu et filtres anti-spam.

4. Faux. L'assurance professionnelle ne couvre pas toujours le risque lié à la perte des données de santé.

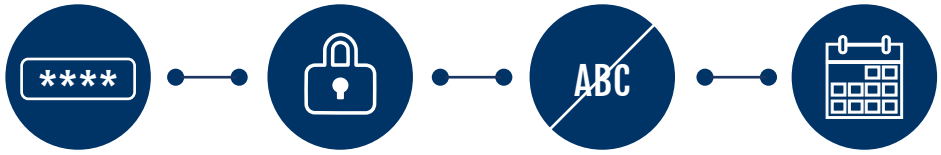
5. Faux. Le stockage de données patients sur son téléphone portable est à proscrire ainsi que les échanges hors messagerie sécurisée.

Vous voulez en savoir plus sur la cybercriminalité et le RGDP ?
Inscrivez-vous à un webinar dédié aux professionnels de santé !

ZOOM SUR LA GESTION DES IDENTITÉS ET DES ACCÈS

Les mots de passe font partie des éléments de sécurité élémentaires à prendre en considération. Il s'agit d'un moyen de gestion des accès simple et peu coûteux pour votre cabinet médical. Toutefois, si le mot de passe ne répond pas à certains critères de sécurité (longueur et complexité, penser à mettre des accents), il peut être facilement compromis. A ce titre, la CNIL partage une nouvelle recommandation sur les mots de passe et fixe les mesures de base à mettre en œuvre.

La CNIL relève 4 points à respecter



- Une authentification par mot de passe avec des critères de longueur et de complexité
- Une authentification sécurisée avec un algorithme public fort
- Un mot de passe qui n'est pas stocké en clair
- Un renouvellement du mot de passe périodique

Quelles sont les erreurs à éviter ?

- Eviter d'utiliser un mot de passe trop simple
- Eviter de conserver votre mot de passe en clair sur un fichier ou votre téléphone
- Evitez de conserver le même mot de passe pendant une longue période

Quels outils de gestion de mots de passe sont recommandés ?

La CNIL propose un outil d'aide à la génération de mot de passe appelé **«PHRASE2PASSE»** pour définir un mot de passe à partir d'une phrase. Le code de l'outil est disponible sous forme d'une extension logicielle en format JavaScript à télécharger sur le site de la CNIL et qui vous permettra de coller le mot de passe dans vos applications.

03

La vulnérabilité des systèmes d'information en santé, même des petits...

?

"Pendant la crise de Covid 19, j'ai beaucoup de collègues qui se sont lancés dans la téléconsultation. Moi non, je ne savais pas vraiment comment faire et je crois qu'en matière de sécurité c'est beaucoup plus contraignant que par téléphone. Au moins au téléphone il n'y a pas de risques de malveillance."

Marie-Pierre, Cardiologue de ville.

Notre point de vue d'expert

"L'augmentation des usages de la télémédecine favorise sans nul doute les actes de malveillance. En pratique, la téléphonie et la téléconsultation peuvent faire l'objet d'actes de malveillance. L'important est de respecter certaines bonnes pratiques. Découvrez nos trucs et astuces à la page suivante."

SÉCURISER L'UTILISATION DU SYSTÈME D'INFORMATION DE SON CABINET MÉDICAL

ÊTRE À L'AISE AVEC SON LOGICIEL MÉDICAL ET SAVOIR L'UTILISER EN TOUTE SÉCURITÉ

En tant que médecin libéral vous utilisez plusieurs fois par jour au moins un logiciel médical pour la gestion des rendez-vous, le suivi de vos patients ou bien la télétransmission des feuilles de soins. Les logiciels sont des outils indispensables au bon fonctionnement d'un cabinet médical ou d'une maison de santé mais cela signifie aussi que plusieurs fois par jour la sécurité des données est menacée.

De quel logiciel parle-t-on ?

- Le logiciel d'aide à la prescription (LAP) médicale : il doit être certifié par la Haute Autorité de Santé (HAS) afin de garantir la conformité et la sécurité de la prescription.
- Le logiciel de télétransmission de feuilles de soins : il doit être conforme au cahier des charges SESAM-Vitale et respecter les conditions de télétransmission des feuilles de soins électroniques. Le but est de garantir l'identité du prescripteur et d'avoir une organisation optimale de la facturation des actes dispensés.
- Le logiciel de gestion de votre agenda et des rendez-vous
- Le logiciel de comptabilité

Quelles sont les précautions à prendre pour la collecte et le traitement des données de santé de vos patients ?

- Premièrement, vous ne devez traiter et collecter les données qu'avec une finalité précise et vous devez par voie de conséquence, éviter de collecter des données inutiles.
- Deuxièmement, les données traitées et collectées doivent être pertinentes.
- Troisièmement, vous devez prendre toutes les mesures nécessaires pour garantir la confidentialité des données de santé de vos patients.
- Enfin, vous devez obligatoirement informer vos patients des objectifs du traitement de leurs données et vous devez conserver les données pendant une durée déterminée (en fonction de vos obligations professionnelles).

Quelles mesures de sécurité adopter en tant que médecin libéral ?

- Vous devez restreindre l'accès des données sensibles aux personnes habilitées.
- Vous devez restreindre également l'accès au logiciel de gestion à un poste et vérifier que l'accès se verrouille lorsqu'il n'est pas utilisé. Pensez toujours à vous déconnecter si vous n'utilisez pas de logiciel.
- Vous devez penser à changer régulièrement de mot de passe, aussi souvent que nécessaire et en cas de doute d'utilisation frauduleuse.
- Vous devez installer et mettre à jour régulièrement un antivirus et un pare-feu.

Vous voulez aller plus loin et évaluer l'hygiène informatique de votre cabinet ?

Faites le point en 6 questions !

Que faire en cas de panne de votre logiciel ?

Les dysfonctionnements de votre logiciel médical peuvent provenir de différentes causes. Il est important d'identifier ces dernières pour résoudre la panne. Cela peut être dû par exemple à la présence d'un virus ou d'un malware, à l'absence d'interopérabilité entre des applications, à un mauvais paramétrage ou bien à une saturation de la mémoire. La liste n'est pas exhaustive. En fonction de la cause de la panne, vous pouvez vous adresser soit à votre éditeur de logiciel soit à votre prestataire informatique. Si vous ne savez pas déterminer la panne, n'hésitez pas à demander une expertise pour identifier la cause du dysfonctionnement.

Et l'hébergement des données de santé ?

Les données de santé font l'objet d'un encadrement réglementaire strict. Leur hébergement est régi par le Code de la santé publique à l'article L 1111-8 : «Toute personne physique ou morale qui héberge des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi médico-social pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil de ces données ou pour le compte du patient lui-même, doit être agréée ou certifiée à cet effet. »

POINT DE VUE D'UN EXPERT EN CYBERSÉCURITÉ

Vincent Trely
Fondateur de l'APSSIS, (association pour la sécurité des systèmes d'information en santé) nous explique pourquoi l'analyse d'impact est une des clés de succès de la cybersécurité.

> " Il faut faire attention à la porosité entre la vie professionnelle et la vie privée. "

Est-ce que lorsqu'un médecin délègue à un prestataire la gestion des données de santé, il est exempt de responsabilité ?

Non. Le médecin reste le responsable des données de santé. Cette responsabilité repose sur deux piliers : le premier ce n'est pas le plus compliqué, signer un contrat avec un hébergeur de données de santé conforme référencé par le ministère de la santé et le deuxième, assurer la partie locale de la confidentialité des accès. Pour ce dernier point, c'est par exemple ne pas utiliser un mot de passe trop simple comme « cabinet », si par exemple il y a 3 médecins et 1 secrétaire médicale, il faut créer 4 comptes nominatif et non un seul accès. Il faut vraiment faire attention à la porosité entre la vie professionnelle et la vie privée. Un médecin devrait avoir un ordinateur personnel pour faire ce qu'il veut et ce n'est surtout pas le même que son ordinateur à usager professionnel avec ses logiciels médicaux.

Selon vous, pourquoi l'analyse d'impact est une clé du succès de la cybersécurité ?

L'AIDP (Analyse d'Impact des Données Personnelles) c'est se poser une heure ou deux et prendre le temps de réflexion sur la nitroglycérine qu'on manipule tous les jours. Les données de santé des citoyens français, il n'y a pas plus secret sur la pyramide de la criticité des données, elles sont au même niveau que les plans de la fusée Ariane ou les plans des centrales nucléaires. Ce sont des données très sensibles. Cela permet de réfléchir aux risques et de faire un travail : si je me fais voler, quelles sont mes obligations, que dois-je faire, comment me prémunir ? Il est 10h30 j'ai déjà vu 11 patients et je n'ai plus d'ordinateur, comment je continue ma journée ? Est-ce que quand le système reprend en fin de journée, j'ai la capacité de le remettre à jour ? C'est de la prévention et de la pré-gestion de crise pour ne pas être en panique quand je rencontre un problème. L'AIPD permet de réfléchir à toutes ces problématiques et évoluer dans le bon sens.

> " Les données de santé sont très convoitées. Les médecins ne sont pas des exploitants informatiques. "

Si vous aviez quelques conseils à donner aux médecins libéraux afin d'améliorer la sécurité des données, ce seraient lesquels ?

Les données de santé sont très convoitées. Il ne s'agit pas simplement de mettre un antivirus sur son poste de travail, c'est avoir deux serveurs, des sauvegardes, chiffrer les données, utiliser des mots de passe complexes, etc. Les médecins ne sont pas des exploitants informatiques et ils n'ont pas à le devenir. Peut-être que l'avenir est dans le cloud, une sorte de coffre-fort numérique avec leurs logiciels, leurs fichiers, leurs ordonnances, etc. Ils se libèrent ainsi de la contrainte de continuité en cas de panne, de vol ou autre. Sinon, je dirais qu'à minima, il faut avoir des logiciels de cabinets médicaux reconnus et labellisés. Il faut également utiliser une messagerie sécurisée, il y a encore beaucoup de médecins qui échangent des données de santé avec un e-mail personnel. Le problème c'est qu'un e-mail ce sont des données qui circulent en clair. On peut donc accéder facilement à une prescription médicale qui est envoyée d'un compte gmail.com par exemple à un compte orange.fr. Sur le darknet on retrouve des centaines d'ordonnances signées et avec le numéro RPPS des médecins, qui ne savent pas qu'on utilise leur ordonnance pour s'approvisionner de méthadone ou toute autre substance. Il faut sécuriser les communications entre professionnels de santé et avec les patients aussi. Toutes les semaines voire tous les jours un établissement de santé, une maison de retraite, un cabinet médical, est infecté et subit une demande de rançon.

> " Il n'y a pas besoin d'une équipe de hackeurs russes pour voler les données des maisons de santé. "

Un mot de la fin ?

Je ne suis pas alarmiste. Je ne prévois pas l'Armageddon numérique, je suis un grand modéré mais j'observe beaucoup le numérique comme une sorte d'épidémiologiste des données numériques. Depuis 3 ou 4 ans on observe une augmentation exponentielle des cyberattaques dans le secteur de la santé. La santé n'a pas encore la même maturité en matière de sécurité que dans l'industrie, les banques, et donc il y a encore beaucoup trop d'opportunités pour les pirates. Contrairement à ce que l'on pourrait penser, il n'y a pas besoin d'une équipe de hackeurs russes pour voler les données des maisons de santé ou des maisons de retraite ! C'est presque de la criminalité low-cost. C'est une vraie réalité et on a aujourd'hui des moyens à disposition pour éviter les ennuis.

LES 10 RÈGLES D'OR POUR RENFORCER SA SÉCURITÉ

1. Identifier tous les risques possibles au sein du cabinet médical
2. Mettre en place un management de la sécurité informatique et une politique de sécurité informatique
3. Acheter un antivirus et firewall
4. Contrôler fréquemment le niveau de sécurité informatique du cabinet médical (mise à jour des mots de passe, contrôle des accès)
5. Être transparent. Pensez à informer votre patientèle sur la collecte et le traitement des données de santé
6. Protéger les données sensibles des patients en respectant le RGPD
7. Tester régulièrement la sécurité informatique et évaluer vos pratiques
8. Se former et être sensibilisé régulièrement (webinaire, formation)
9. Faire appel à un accompagnement dès que le besoin s'en fait ressentir
10. Être dans une démarche d'amélioration continue

Pas certain de savoir par où commencer ? Ne restez pas seul avec vos questions,
faîtes appel à un expert pour un bilan gratuit !
De là, vous saurez ce que vous devez faire :-)

04

Les bonnes pratiques pour se prémunir et protéger son cabinet médical des cyberattaques !

"Je suis médecin de campagne au fin fond de la Bourgogne. Je ne pense pas que les données de santé de mes trente patients intéressent les hackeurs. Je me concentre sur mon cœur de métier et ce depuis des dizaines d'années. Je n'ai jamais eu le moindre problème. D'ailleurs c'est plutôt les gros CHU qui sont victimes de cyberattaques."

Frédéric, Médecin de campagne.

Notre point de vue d'expert

"Ce n'est pas tout à fait correct, d'ailleurs on vous explique comment devenir cyber-résilient au sein de votre cabinet médical !"

DEVENEZ CYBER-RÉSILIENT !

La cyber-résilience informatique de quoi s'agit-il ?

La cyber-résilience c'est admettre l'existence et la possibilité de survenue de cyber incidents dans un monde informatique vaste, en constante évolution. Surtout, c'est savoir faire face aux menaces lorsqu'elles surviennent.
Le but de cette approche est non pas la fatalité mais plutôt la constante recherche de la sécurité informatique afin de réduire l'impact d'une cyber-attaque sur votre activité médicale. La cybersécurité devient alors une partie intégrante de la cyber-résilience.
En tant que médecin, vous devrez bénéficier de l'accompagnement d'experts en sécurité informatique pour vous aider à définir une stratégie de sécurité informatique efficace en cas d'attaque.

Comment mettre en place une stratégie de cyber-résilience ? Quelles sont les étapes ?

1. Comprendre la vulnérabilité et les menaces auxquelles on peut être confronté en tant qu'usager informatique, traitant et collectant des données de santé
2. Identifier les risques
3. Vérifier votre conformité RGPD et tester régulièrement votre sécurité afin de prévenir les risques
4. Développer un plan d'action en amont afin de définir vos priorités face à une cyber attaque et vous relever en garantissant une continuité d'activité

Pourquoi souscrire à une cyber-assurance ? Quels avantages ?

La cyber-assurance est encore très peu connue et pourtant elle couvre vos risques liés au cyberspace. Elle est primordiale car tous vos risques ne sont pas assurés par votre assurance professionnelle !

En tant que professionnel de santé libéral, vous pouvez vous sentir dépassé et perdu face à toutes les responsabilités liées à votre métier et aux données sensibles que vous traitez et collectez. En cas d'attaques ou de fraude contre votre cabinet médical, c'est votre responsabilité qui est engagée et il pourra vous être imputé une atteinte aux données personnelles et confidentielles, à la sécurité de votre réseau, ou à d'autres manquements comme l'absence d'information à vos usagers sur le traitement de leurs données. La cyber-assurance permet d'être accompagné en toute sérénité par des experts lors de la survenue de cyber-attaques afin d'affronter tous les défis financiers et juridiques.

Personne n'est à l'abri d'une faille, une assurance peut s'avérer utile. Y avez-vous déjà pensé ? Pourquoi souscrire à une assurance ? **Réponse en vidéo**

13 ÉTAPES VERS LA CYBER-RÉSILIENCE

L'INDISPENSABLE CHECK-LIST

1. Vous disposez d'un antivirus et d'un firewall à jour
2. Vous sauvegardez régulièrement vos données
3. Vous avez informé vos patients sur le traitement et la collecte de leur données
4. Vous avez vérifié votre conformité au RGPD et au référentiel relatif aux traitements de données à caractère personnel destinés à la gestion des cabinets médicaux et paramédicaux
5. Vous avez un plan d'amélioration continue
6. Vous disposez d'une cyber-assurance
7. Vous avez créé des accès restreints à votre logiciel de gestion médicale
8. Vous changez régulièrement de mots de passe et ils sont conformes aux exigences de la CNIL
9. Vous avez réalisé votre analyse d'impact
10. Vos données sont hébergées chez un hébergeur de santé agréé
11. Vous êtes formé à la cybersécurité
12. Vous tenez un registre de cybersécurité
13. Votre cabinet est accompagné par des experts sécurité

QUE FAIRE EN CAS DE CYBERATTAQUE AU SEIN DE MON CABINET MÉDICAL ? 6 RÈGLES POUR ÊTRE EFFICACE !

Déconnectez-vous d'internet rapidement, que ce soit en filaire ou en wifi !

Repérez les signes
Vous recevez des spams en grande quantité ? Votre ordinateur est ralenti ? Votre antivirus vous notifie des messages d'alerte ? Vos logiciels ne démarrent plus normalement ?

Identifiez le problème
S'agit-il d'un virus informatique ? D'une fraude ? Déclenchez une recherche anti-virus pour vérifier si votre poste de travail est infecté et restaurer votre appareil si besoin

Faites appel à votre expert sécurité
et décrivez lui le problème afin qu'il vous indique la meilleure conduite à tenir

Modifiez systématiquement tous vos mots de passe

Prévenez vos patients

Portez plainte

SOURCES

Arpagian Nicolas, « Définition et historique de la cybersécurité », dans : Nicolas Arpagian éd., La cybersécurité. Paris cedex 14, Presses Universitaires de France, « Que sais-je ? », 2015, p. 7-30. URL : https://www.cairn.info/la-cybersecurite--9782130652199-page-7.htm

APSSIS, https://www.apssis.com consulté le 25 juillet 2020

LET, Communiqué de presse du 30 Juin, https://www.lesentel.org/communique-de-presse/

AMELI, https://www.ameli.fr/fileadmin/user_upload/documents/20200331_-CP_Teleconsultations_Covid_19.pdf consulté le 2 juillet 2020

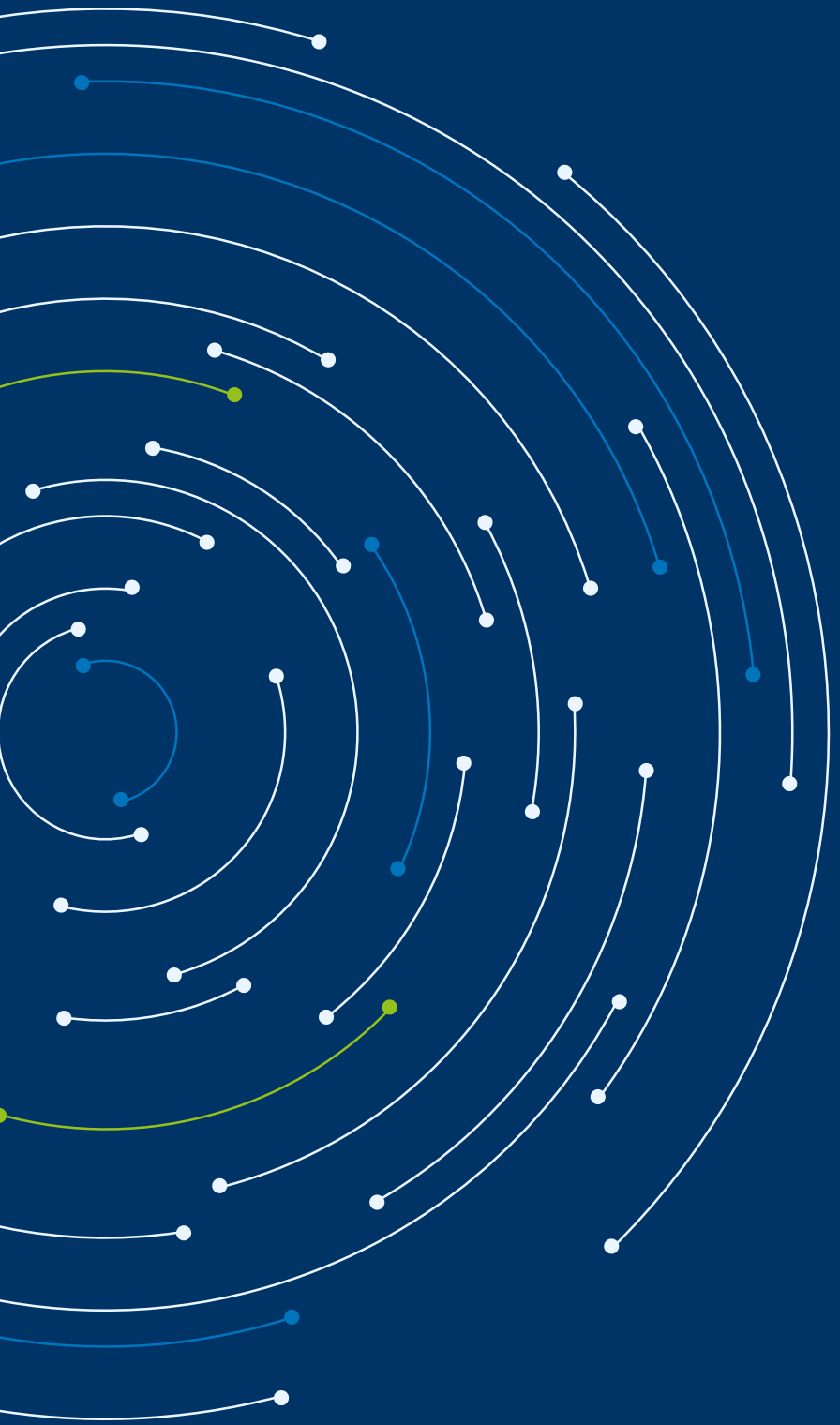
CAIRN, https://www.cairn.info/revue-securite-et-strategie-2012-4-page-74.htm, consulté le 27 juillet 2020

OMS, https://www.who.int consulté le 21 juillet 2020

ANSSI, https://www.ssi.gouv.fr consulté le 20 juillet 2020

CNIL, https://www.cnil.fr/fr consulté le 20 juillet 2020 https://www.cnil.fr/sites/default/files/atoms/files/referentiel_-_traitements_dans_le_domaine_de_la_sante_hors_recherches.pdf, consulté le 29 juillet 2020

TICSANTE, https://www.ticsante.com consulté le 21 juillet 2020



CGM SECURE

Protection des Données Patient

Merci pour votre intérêt et si vous souhaitez aller plus loin, contactez nos conseillers en cybersécurité !

01 47 16 20 00 (prix d'un appel local)
info@cgmnet-fr.cgm.com

POUR EN SAVOIR PLUS

cgm.com/fr/cgm-secure