E-SANTÉ (/ACTUS-PRO/E-SANTE)

Médecins libéraux : comment vous prémunir des cyberattaques

6

Par Aveline Marques le 27-02-2021

La multiplication des cyberattaques dont les hôpitaux sont la cible et la récente fuite des informations médicales de 500.000 patients démontrent la forte valeur accordée aux données de santé. Si les établissements sont indéniablement des cibles stratégiques, les cabinets libéraux ne sont pas à l'abri. A l'heure où se multiplient les échanges numériques entre acteurs de soins et l'intervention de "tiers" (plateformes de télémédecine ou de prise de rendez-vous), les médecins libéraux doivent impérativement relever le niveau de sécurité des données et abandonner certaines "mauvaises habitudes".

Des milliers d'images médicales accessibles en ligne, à la portée du premier venu. Pour avoir "insuffisamment protégé les données personnelles de leurs patients" et s'être "affranchis des principes élémentaires en matière de sécurité informatique", deux médecins libéraux ont été condamnés par la Commission nationale informatique et libertés (Cnil) à verser des amendes de 3.000 et 6.000 euros en décembre dernier. Une sanction rare sur laquelle la formation restreinte de la Cnil a voulu communiquer (https://www.cnil.fr/fr/violations-de-donnees-de-sante-la-cnil-sanctionne-deux-medecins) "pour alerter les professionnels de la santé sur leurs obligations et la nécessité de renforcer leur vigilance sur les mesures de sécurité apportées aux données personnelles qu'ils traitent".

Car les médecins libéraux sont, au même titre que les hôpitaux, les entreprises ou encore les collectivités, soumis au Règlement général sur la protection des données (RGPD), entré en application en France en mai 2018. Les informations notées dans les dossiers patients (papier ou informatisés), collectées pour la prise de rendez-vous, pour la téléconsultation ou dans le cadre de la gestion du cabinet (fournisseurs, employés) constituent en effet des données personnelles dès lors qu'elles se rapportent à "une personne physique identifiée ou identifiable", rappelle le guide pratique édité par la Cnil et l'Ordre des médecins (https://www.cnil.fr/sites/default/files/atoms/files/guide-cnom-cnil.pdf) en juin 2018.

>> Lire aussi : Fuite inédite de données médicales : ce que l'on sait
(https://www.egora.fr/actus-pro/faits-divers-justice/65540-fuite-inedite-de-donnees-medicales-ce-que-l-on-sait)

Usurpation d'identité

Les données de santé sont d'autant plus *"sensibles"* qu'elles touchent *"à l'intime"*, relève Benjamin Vialle, chef du service des contrôles RH, santé et affaires publiques de la Cnil. Et qu'elles sont aujourd'hui particulièrement ciblées par les pirates informatiques : depuis le début de l'année 2021, chaque semaine, un hôpital français est la cible d'une cyberattaque. Quand ils ne paralysent pas le système informatique avec un rançongiciel, entravant...

la bonne marche des soins, les pirates dérobent les données des patients ou des soignants pour les revendre sur le Dark web, où elles valent plus chères que les données bancaires. Les données des patients (nom, prénom, date de naissance, adresse, numéro de sécurité sociale, ordonnances…) permettent en effet d'usurper une identité pour frauder, tandis que les données des membres du personnel permettent d'a[illegible]r aux systèmes informatiques des établissements ou de légitimer un faux professionnel en utilisant u[illegible]e de diplôme, par exemple. Tout récemment, un fichier contenant les informations personnelles de

près de 500.000 personnes, volées à un groupe de laboratoires, a été diffusé sur le web (https://www.egora.fr/actus-pro/e-sante/65521-medecin-traitant-etat-de-sante-medicaments-les-donnees-de-500000-patients) à la suite d'une dispute entre hackers. Outre les coordonnées et le numéro de sécurité sociale, il comprend aussi des informations sur le groupe sanguin ou l'état de santé (stérilité, VIH…) des patients.

Même si elles ne tombent pas dans de mauvaises mains, des données de santé trop largement accessibles peuvent porter préjudice aux personnes concernées. C'est l'un des problèmes les plus fréquemment rencontrés par la Cnil lors de ses contrôles dans les hôpitaux : *"les données des patients sont souvent trop accessibles, du fait d'une définition de l'habilitation trop large",* pointe Benjamin Vialle. Si un professionnel de santé intervenant dans la prise en charge d'un patient peut avoir un accès spécifique à son dossier, le personnel administratif d'un autre service, par exemple, ne devrait pas pouvoir le consulter. *"Quand vous êtes hospitalisé en psychiatrie pour burn out, vous n'avez pas forcément envie que des collègues puissent accéder à votre dossier",* illustre le chef de service de la Cnil. Même règle dans les cabinets médicaux : une secrétaire médicale ne devrait pas avoir un accès global au dossier du patient.

> **>> Lire aussi : Pirate vend 10 millions de dossiers médicaux pour 1 million de dollars** (https://www.egora.fr/actus-pro/conditions-d-exercice/16499-pirate-vend-10-millions-de-dossiers-medicaux-pour-1-million-de)

De manière générale, le RGPD commande aux médecins de ne recueillir dans le dossier patient que les informations strictement nécessaires à la prise en charge et à la gestion du cabinet, rappelle le guide de la Cnil et de l'Ordre. En revanche, "toute information qui serait sans lien avec l'objet de la consultation du patient ou qui ne serait pas indispensable au diagnostic ou à la délivrance des soins doit être exclue", insiste les deux institutions. Oui à l'origine ethnique "si elle a une influence particulière sur une pathologie ou un traitement". Non à son orientation sexuelle ou à sa religion, si ces informations sont sans incidence. De même, pour la prise de rendez-vous, les motifs de consultation n'ont pas à être renseignés si la consultation ne nécessite pas de préparation au préalable ou la réservation d'outils spécifiques, insiste le guide.

“Mauvaises habitudes” des médecins

Mais surtout, l'ensemble de ces données doivent être davantage sécurisées. *"Un mot de passe sur l'ordinateur, ce n'est pas suffisant",* pointe Fabien Fernandez, directeur d'Asklépian, société qui s'est spécialisée dans...

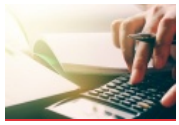
la protection des données, notamment dans le domaine de la santé. Délégué à la protection des données (DPD) certifié par la Cnil, ce dernier ne peut que constater les *"mauvaises habitudes"* prises par les professionnels libéraux : envoyer une image médicale à un confrère via Whatsapp, communiquer avec ses patients ou ses confrères via une messagerie standard type Gmail plutôt qu'avec une messagerie sécurisée, laisser les documents médicaux dans le dossier "téléchargements" de l'ordinateur plutôt que sur un serveur sécurisé et crypté, se contenter de tout sauvegarder sur un disque dur non protégé en cas de perte ou de vol, ouvrir un accès à des centaines de professionnels (pratique fréquente des cabinets dentaires ou de radiologie) ou encore remettre des résultats médicaux au vu et au su de tous… Asklépian a ainsi été contacté par une patiente scandalisée de voir son médecin généraliste laisser sur une table du sas d'entrée de son cabinet une enveloppe à son nom mentionnant son contenu : le résultat d'un test VIH. *"Elle voulait porter plainte",* se souvient Fabien Fernandez. La Cnil reçoit ainsi chaque année 13 à 14.000 plaintes, qui débouchent parfois sur des contrôles. Mais ce n'est pas le cas des deux médecins sanctionnés en décembre : la *"fuite"* de ces données médicales avaient été révélée dans la presse, précise Benjamin Vialle.

> **>> Lire aussi : Un médecin pirate les ordinateurs de ses confrères : 4 mois de prison avec sursis** (https://www.egora.fr/actus-pro/faits-divers-justice/38759-un-medecin-pirate-les-ordinateurs-de-ses-confreres-4-mois-de)

La plainte d'un patient peut néanmoins donner lieu à une condamnation ordinale : en 2009, un médecin généraliste a écopé de trois ans d'interdiction temporaire d'exercice (dont deux avec sursis) pour avoir publié sur son site des photos avant/après non floutées d'une patiente sur laquelle il avait pratiqué une intervention esthétique, et ce, sans avoir recueilli son consentement. L'Ordre rappelle ainsi dans son guide que les patients doivent être informés du recueil de données et de sa finalité.

Manque de temps, méconnaissance ou négligence ? Pour la Cnil, qui a fait de la protection des données de santé, l'une de ses thématiques prioritaires en 2020, il n'y a pas de *"volonté délibérée"* des médecins libéraux de ne pas respecter le RGPD. Mais il indéniable que ces derniers doivent *"relever le niveau de sécurité des données de santé",* insiste Benjamin Vialle. Car ils ne sont pas à l'abri des cyberattaques. *"On a l'exemple d'un médecin qui un matin, arrivant à son cabinet, a constaté que tout était crypté,* se souvient Fabien Fernandez, d'Asklépian. *Il s'est retrouvé dans l'incapacité d'exercer : il n'avait plus accès à son planning, ni à l'historique de suivi de ses patients. Pour ces patients qui avaient peut-être attendu ce rendez-vous plusieurs mois, ce n'est pas de chance. Et pour le médecin, ça représente une perte d'activité."* Que faire dans ce cas-


professionnelle


PRÉVOYANCE
Faut-il transférer son Madelin vers un PER ?


RÈGLES D'EXERCICE
Un médecin peut-il être interdit d'exercice en cas d'infirmité ou de troubles pathologiques ?


RÈGLES D'EXERCICE
Les droits et devoirs du médecin retraité

là? *"Débranchez votre ordinateur d'internet et du réseau local pour éviter qu'il contamine tout le système et déconnectez tous les appareils susceptibles d'être infectés. Mais n'éteignez...*

pas votre ordinateur : ça efface les traces de la cyberattaque", conseille le DPD.

> **>> Lire aussi : Un médecin peut-il communiquer à ses patients son adresse email?** (https://www.egora.fr/gestion-cabinet/juridique/relation-medecinpatient/un-medecin-peut-il-communiquer-a-ses-patients-son)

Pour prévenir et se relever rapidement de ce type d'attaques, le directeur d'Asklépian insiste : *"Le médecin doit avoir la maitrise de son système informatique. Il faut mettre les barrières au bon endroit : les barrières techniques, mais aussi les barrières organisationnelles. 80% des violations viennent d'une erreur humaine",* souligne-t-il. Pour cela, 5 à 10% du budget doit être consacré à la sécurisation des données, selon une estimation courante. Chez Asklépian, le service est facturé entre 1.000 et 1.500 pour une session collective de conseils, 3.000 euros pour une prestation de conseils individuelle et jusqu'à 6.000-12.000 euros (en fonction de la taille du cabinet) pour un accompagnement clé en main sur neuf mois. S'ajoute ensuite le coût des différentes mesures de protection mises en œuvre – 1.000 à 1.500 pour un cabinet avec trois ordinateurs et une ouverture restreinte vers l'extérieur, estime Fabien Fernandez. De quoi y consacrer une bonne partie du forfait structure… *"Le RGPD précise que l'on doit mettre les moyens techniques et organisationnels adéquats et cohérents… c'est-à-dire avec le chiffre d'affaires",* souligne-t-il. Si les pirates ciblent les professionnels de santé libéraux, ce n'est pas seulement parce que les données de santé ont de la valeur mais aussi parce que ces derniers ont les moyens de payer les rançons et ne peuvent se permettre de suspendre leur activité trop longtemps. En matière de médecine comme d'informatique, mieux vaut prévenir que guérir.

Données personnelles : les 10 commandements du médecin libéral

1. Limiter les informations collectées au strict nécessaire et les utiliser conformément aux finalités définies
2. Restreindre l'accès aux dossiers patients et chiffrer les données personnelles avec un logiciel adapté
3. Sécuriser le système informatique (mot de passe de 12 caractères avec chiffres, majuscules, et caractères spéciaux, verrouillage de session au bout de 30 minutes, anti-virus et pare-feu à jour, authentification forte ou via la CPS…) et tous les appareils connectés
4. Informer les patients du recueil de leurs données personnelles et de sa finalité (modèle d'affiche ici (https://www.cnil.fr/fr/rgpd-le-conseil-national-de-lordre-des-medecins-et-la-cnil-publient-un-guide-pratique-lattention-des))
5. Tenir un registre des activités de traitement (modèle ici (https://www.cnil.fr/fr/rgpd-le-conseil-national-de-lordre-des-medecins-et-la-cnil-publient-un-guide-pratique-lattention-des))
6. Utiliser une messagerie sécurisée, ou à défaut crypter les pièces jointes envoyées par une messagerie standard
7. Ne pas utiliser des appareils personnels (PC portable, smartphone, tablette) à des fins professionnelles ou a minima, ne pas y stocker d'informations médicales
8. Effectuer des sauvegardes régulières (au minimum hebdomadaires) et sécurisées
9. S'assurer de la conformité des prestataires (plateformes de prise de rendez-vous, de télémédecine…) en matière de protection des données
10. Notifier toute violation des données à la Cnil