LA CYBERSÉCURITÉ : ENJEUX ET PRÉVENTION POUR LES OPHTALMOLOGISTES

STÉPHANIE BARRUS-MARQUETTE
(chef de produit assurance dommage/ MACSF)
JEAN PAUL TAVIN (SNOF)

Mme S. Barrus Marquette : Ces derniers mois, nous avons beaucoup entendu parler de cyberattaques dans les établissements de santé, notamment au centre hospitalier Sud-Francilien de Corbeil-Essonnes ou au centre hospitalier de Versailles… cette médiatisation cache cependant une réalité : celle que les plus petites structures de type cabinets ou centres ophtalmologiques sont elles aussi touchées.

POURQUOI SE PROTÉGER DES ATTAQUES ?

Le RGPD (Règlement Général sur la Protection des Données) encadre le traitement des données personnelles sur le territoire de l'Union Européenne depuis 2018. Il prévoit que toutes les organisations publiques et privées, qui traitent des données personnelles pour leur compte ou non, **sont responsables** dès qu'il y a violation des données personnelles (destruction, perte, divulgation ou accès non autorisé).

Une « donnée personnelle » est à comprendre de façon large comme « toute information se rapportant à une personne physique identifiée ou identifiable ».

Les médecins sont doublement concernés car la protection des données personnelles s'articule avec leur secret professionnel.

Outre le respect du cadre réglementaire, une cyberattaque génère :

- **Interruption du système d'informations**
  - Gestion de l'incident et traitement correctif de la faille de sécurité
  - Exposition à un chantage, à une demande de rançon
  - Pertes d'exploitation lié à un blocage des systèmes
- **Perte des données personnelles de la patientèle**
  - Mise en jeu de votre responsabilité civile vis-à-vis des patients :
    - Le RGPD oblige en effet à notifier à la CNIL et aux patients (!) toute compromission des données
    - Risque de poursuites de vos patients (demande de réparation du préjudice moral ou financier)
  - Risque d'image et d'atteinte à la réputation
  - Sanctions pénales et ou administratives
- Et surtout des **pertes financières**

COMMENT SE PROTÉGER ?

- La prévention
- La prévention
- Et… la prévention !

1. Maîtriser l'accès physique aux équipements informatiques

En premier lieu, il peut être considéré comme essentiel de sécuriser l'accès aux outils informatiques qui hébergent les données de vos patients.

Vous devez vous assurer que votre cabinet ou centre est bien protégé contre les vols en installant par exemple un système de sécurité renforcée sur vos portes extérieures et fenêtres ou en faisant appel à une société de télésurveillance. Veillez également à ce que vos équipements informatiques restent inaccessibles au public et surtout ne pas oublier de verrouiller votre poste de travail lorsque vous vous absentez de votre bureau.

2. Respecter les règles d'utilisation de votre Carte de Professionnel de Santé

En tant que professionnel de santé, vous disposez d'une carte CPS vous permettant d'échanger des données ou de rechercher des informations dans le DMP (dossier médical partagé) directement depuis votre ordinateur.

Cette carte est personnelle et ne peut en aucun cas être cédée à une tierce personne. Prenez soin de l'avoir toujours sur vous ou rangée dans un lieu sûr pour éviter les risques de perte ou de vol. Son code PIN doit être gardé secret et l'ensemble des documents en faisant mention doit être détruit.

3. Sécuriser vos mots de passe informatiques

Un manque de rigueur dans la gestion des mots de passe est une des causes les plus souvent identifiées lors d'une intrusion informatique.

Les mots de passe doivent respecter certaines règles pour ne pas être facilement découverts par les outils à la disposition des pirates. Les spécialistes recommandent de les penser de façon à ce qu'ils soient :

- Longs d'au moins 12 caractères
- Composés de minuscules, majuscules, chiffres et signes spéciaux
- Mémorisés et non notés sur un support accessible à un tiers
- Uniques pour chaque compte

Dès que cela est possible, l'authentification à double facteurs doit également être utilisée (application sur le téléphone par exemple). Elle permet de se prémunir contre le vol de mot de passe : ainsi, le seul mot de passe ne suffit plus pour accéder au compte et aux données.

4. Penser à sauvegarder vos données

L'ensemble de vos données est à sauvegarder régulièrement, afin de pouvoir être facilement récupéré en cas d'incident.

Ce risque numérique est d'autant plus important que les cyberattaques de type rançongiciel - qui ont la particularité de chiffrer vos données et de les rendre inutilisables - sont de plus en plus fréquentes dans le monde de la santé.

Les enregistrements sont réalisés sur des supports amovibles, déconnectés du poste informatique entre deux sauvegardes, et conservés dans un lieu sécurisé.

En cas de sauvegarde externe confiée à un organisme hébergeur de données, ce dernier doit être certifié HDS (Certification Hébergeur de Données de Santé). L'Agence du numérique en santé (ANS) recense plus de 140 hébergeurs certifiés, dont des éditeurs de logiciels, des sociétés spécialisées dans l'hébergement, des groupes de cliniques et des CHU.

5. Utiliser une messagerie sécurisée

Il vous arrive certainement d'envoyer des documents concernant vos patients à des confrères ou à des établissements de santé depuis votre messagerie professionnelle ?

Sachez qu'il existe des outils de messagerie sécurisée de santé, qui permettent de protéger vos échanges et de faire en sorte que ces données à caractère personnel et confidentiel ne soient pas interceptées et utilisées à des fins malveillantes.

6. Respecter les principes du règlement général sur la protection des données (RGPD)

Dans le cadre du RGPD, les professionnels de santé sont tenus de garantir la confidentialité des données de santé de leurs patients. Au quotidien comme en cas de partage de cabinet ou d'activité, ils doivent veiller à ce que chaque soignant de la structure ne puisse accéder qu'aux données qui lui sont nécessaires.

Cela vaut également pour l'ensemble de ses partenaires : prestataire de télémaintenance, plateforme de prise de rendez-vous...

Une maîtrise absolue de la sécurité des systèmes d'informations n'est jamais acquise ! Outre la prévention des risques, il existe des solutions assurantielles pour exercer sereinement son activité.

Dr JP Tavin : En conclusion et vous l'aurez compris le risque existe, les précautions à prendre sont de bon sens et vous les connaissez. Reste à les mettre systématiquement en pratique. Ce genre d'incident n'arrive pas qu'aux autres, c'est un risque fort. L'attaque informatique désorganise la structure pour plusieurs jours, elle génère une perte d'exploitation, un risque de poursuites de la part des patients, un risque de sanction pénale ou ordinale. L'attaque informatique est génératrice de stress bien évidemment. Tout ça n'est pas anodin et doit être présent dans nos esprits. Prévention !

Mais rien n'est jamais totalement sûr dans ce monde de pirates. Alors pour aller plus loin que la prévention, il existe des solutions assurantielles, pour vous conseiller sur les mesures de prévention à adopter et pour couvrir les risques de ce type d'attaque permettant ainsi de gérer au mieux cette problématique. Par exemple, la MACSF, propose un pack Cyber intégré dans le contrat multirisque professionnel.

Plus d'information sur
https://www.macsf.fr/nos-produits-services/vie-professionnelle/assurance-cyber-risques