DOC
LE RENDEZ-VOUS
DES MÉDECINS
VAUDOIS

Rôle des associations professionnelles

« Avec quelques règles d'hygiène numérique de base, on peut déjà diminuer les risques »

Aucun médecin n'a oublié la cyberattaque de mars 2022 qui a visé de nombreux cabinets romands, principalement dans le canton de Neuchâtel. En réaction immédiate, le Dr Dominique Bünzli, médecin de famille et président de la Société Neuchâteloise de Médecine, avait fait part de ses inquiétudes face à la vulnérabilité des données patient-es et de la nécessité de les sécuriser dans les meilleurs délais. Il répond à nos questions.

Quels sont les enjeux et conséquences en cas de cyberattaques ?

Juridiquement, les données médicales sont considérées comme des données sensibles et le médecin est le maître du fichier en vertu de la Loi sur la protection des données (LPD). C'est donc lui qui est responsable de la sécurité des données contre les traitements non autorisés. Il doit aussi en garantir l'intégrité en respectant les délais de conservation (voir page 11). Les enjeux sont multiples : arrêt de l'activité avec impacts potentiels sur la santé des patient-es et conséquences sur l'image et la réputation. Il y a aussi un risque juridique avec un-e patient-e qui se retournerait contre son médecin en cas de préjudice. Finalement, dans la nouvelle loi LPD prévue pour 2023, des amendes sont prévues. En cas de cyberattaque, un enjeu important consiste à communiquer de manière transparente et proactive, ce qui nécessite une préparation soigneuse.

Quel rôle peuvent jouer les associations professionnelles pour mettre en place une vraie infrastructure de sécurité ?

Cela dépend du niveau et de la taille de l'association. Petite, son rôle principal est de sensibiliser les membres, dès leur adhésion, en leur transmettant par exemple des sources utiles (documentation FMH et guide cybersécurité de la SNM). Avec quelques règles d'hygiène numérique de base, on peut déjà diminuer les risques. Les sociétés cantonales peuvent aussi proposer de clarifier les rôles, les responsabilités et la relation avec les prestataires informatiques. Pour des sociétés plus grandes et pour aller plus loin, elles pourraient développer des services accessibles à des tarifs préférentiels comme des audits ou des contrats avec certaines assurances cybersécurité. En cas d'attaque, la société cantonale devrait soutenir les membres touchés, notamment à travers la communication.

Quelles nouvelles prestations les sociétés cantonales pourraient-elles offrir à leurs membres ?

Elles pourraient réfléchir à la mutualisation des moyens pour atteindre des niveaux de sécurité type bancaire (p.ex. monitoring humain), en s'approchant d'infrastructures informatiques plus importantes, cantonales ou hospitalières. Une piste future serait aussi d'intégrer la cyberprotection au sein des communautés DEP (dossier électronique du patient). Cette option n'est cependant pas évidente en pratique car nous avons des infrastructures informatiques hétérogènes. Ces démarches doivent bien sûr être discutées par les comités voire approuvées par les membres, car cela a des conséquences financières sur les cotisations.

Se pose la question d'un label ou d'une accréditation des fournisseurs avec des conditions strictes à remplir…

Cela fait partie des mesures pour améliorer la sécurité. Un audit – avec ensuite la possibilité d'un label – donne une idée de sa sécurité mais uniquement à un moment donné. Cela n'empêche pas de continuer à faire évoluer sa sécurité, avec des mises à jour par exemple. Concernant l'accréditation des fournisseurs, c'est aussi une piste. Aujourd'hui, on peut déjà utiliser les contrats-types édictés par la FMH pour les

DOC
LE RENDEZ-VOUS
DES MÉDECINS
VAUDOIS

prestataires Cloud.

Propos recueillis par la rédaction