FMH SERVICES

Prendre la protection des données au sérieux et instaurer la confiance

Les conséquences de la perte et de la manipulation de données pouvant être particulièrement graves dans le secteur de la santé, des mesures de sécurité sont nécessaires à tous les niveaux.

La numérisation progresse inexorablement dans le secteur de la santé, avec ses avantages et ses inconvénients. Les processus peuvent être organisés de manière plus efficace et donc, accélérés. Les outils numériques sont également devenus incontournables dans les hôpitaux et les cabinets médicaux. La numérisation croissante augmente toutefois le risque de cyberattaques.

Les données relatives à la santé des personnes font partie des «données personnelles sensibles» et exigent en conséquence une très bonne protection, contre notamment les modifications non autorisées, la destruction et l'utilisation abusive. Des informations erronées ou manquantes peuvent avoir de graves conséquences et mettre en danger la santé, voire la vie dans le pire des cas [1] .

Mesures de sécurité à tous les niveaux: comportement, technique et organisation
Seule une approche intégrale de la protection des données sensibles relatives à la santé permet d'assurer la protection la plus complète possible. Cette approche prévoit d'aborder le sujet sous différents angles. Les mesures de sécurité peuvent être classées en trois catégories: comportementales, organisationnelles et techniques.

L'utilisation de mots de passe longs et complexes entre par exemple dans le cadre des mesures comportementales. Pour éviter de devoir les apprendre par coeur, il est recommandé de recourir à un gestionnaire de mots de passe sécurisé. Un tel programme permet de sauvegarder et de conserver les mots de passe en toute sécurité. L'utilisation de l'authentification à deux facteurs offre une protection supplémentaire, l'utilisateur devant se connecter avec un deuxième facteur en plus du mot de passe. Les applications d'authentification (comme l'application HIN Authenticator) ou un fichier d'identité déposé, comme c'est le cas par exemple dans le client HIN, constituent un deuxième facteur possible. Dans le cas où un mot de passe est piraté par des tiers non autorisés, ces derniers n'auront pas accès au compte en question, car il leur manque le deuxième facteur. Outre la protection des comptes personnels, il est important de toujours transmettre les données sensibles de manière cryptée (par exemple avec HIN Mail). Les e-mails non cryptés comportent des risques importants, car le contenu du message peut être intercepté et consulté par des tiers non autorisés. La confidentialité d'un e-mail non crypté est ainsi souvent comparée à celle d'une carte postale.

La mise à jour permanente de tous les systèmes informatiques compte parmi les principales mesures techniques. Des sauvegardes régulières et sécurisées permettent de récupérer les données perdues en cas de cyberattaque. L'importance de sauvegardes régulières a par exemple été démontrée lorsque le groupe Hirslanden a été victime d'un rançongiciel à l'automne 2020 [2] . Les données cryptées ont pu être récupérées grâce à une sauvegarde, et les soins aux patients n'ont connu aucune perturbation.

Des mesures organisationnelles peuvent également aider à augmenter massivement la protection des données sensibles. Les risques peuvent être minimisés grâce à des directives relatives à la sécurité et à des processus contrôlés. Il s'agit par exemple de déterminer les responsabilités ou de restreindre les autorisations. Les supérieurs qui montrent l'exemple peuvent motiver les collaborateurs à prendre la question de la protection des données au sérieux. Complétée par une formation régulière des collaborateurs sur le thème de la protection des données et de la sécurité informatique, il en résulte une sensibilisation accrue qui, à long terme, se répercute positivement sur le traitement des données sensibles.

Sensibiliser aux dangers par une formation ciblée
Les mesures techniques sont importantes pour la protection des données sensibles, mais le comportement humain est un facteur tout aussi important. Une personne consciente des dangers de la cybercriminalité peut y faire face avec plus de sécurité et même, dans certaines circonstances, intervenir là où la technique échoue. Pour sensibiliser les collaborateurs au thème de la sécurité des

données, il est recommandé de leur faire suivre une formation régulière et ciblée. L'accent ne doit pas être mis sur la simple transmission d'informations, mais sur la sensibilisation à long terme des dangers potentiels. Une formation à la protection des données pose une base solide pour que chacun soit conscient de ses responsabilités et les assume dans son travail quotidien.

Dans son rapport explicatif relatif à la nouvelle loi sur la protection des données (nLPD), l'Office fédéral de la justice (OFJ) souligne lui aussi expressément la pertinence des formations et des conseils [3] . En effet, le Conseil fédéral estime que la mise en oeuvre et l'efficacité de la sécurité des données dépendent notamment de l'application correcte par les personnes impliquées des mesures prévues en matière de sécurité informatique et de protection des données. Des formations et des conseils permettent de minimiser les risques de violation de la sécurité des données, par exemple en utilisant de manière réfléchie les pièces jointes ou les liens potentiellement dangereux des e-mails.

Prendre la protection des données au sérieux et instaurer la confiance
Les patients sont en droit d'attendre des personnes responsables de leur prise en charge un traitement soigneux et donc un comportement légitime en ce qui concerne le traitement de leurs données. Les professionnels de la santé sont tenus de respecter le secret médical et sont soumis à la loi sur la protection des données. Un traitement des patients de haute qualité implique donc, entre autres, la prise en considération constante des aspects de la protection des données. Les médecins qui indiquent à leurs patients qu'ils assument leur responsabilité en matière de protection des données (par exemple avec le label HIN) contribuent à renforcer le lien de confi ance entre le médecin et le patient.

Sources
[1] Centre national pour la cybersécurité NCSC, rapport semestriel 2020/2, 11.05.2021, https://www.ncsc.admin.ch/ncsc/fr/home/dokumentation/berichte/lageberichte/halbjahresbericht-2020-2.html
[2] Neue Zürcher Zeitung, «Cyberattaque contre le groupe Hirslanden: la crise sanitaire rend les hôpitaux particulièrement vulnérables aux menaces», 25.11.2020, https://www.nzz.ch/schweiz/cyberangriffe-auf-die-hirslanden-gruppe-die-spitaeler-sind-wegen-der-pandemie-besonders-anfaellig-fuer-erpressungen-ld.1587386
[3] Office fédéral de la justice (OFJ), «Révision totale de l'ordonnance relative à la loi fédérale sur la protection des données», rapport explicatif relatif à la procédure de consultation, 23.06.2021, https://www.bj.admin.ch/dam/bj/fr/data/staat/gesetzgebung/datenschutzstaerkung/vdsg/vn-ber.pdf

A propos
Jona Karg, Responsable de la formation

Health Info Net AG
Seidenstrasse 4
8304 Wallisellen
Téléphone 0848 830 740
jona.karg@hin.ch
www.hin.ch