DOC
LE RENDEZ-VOUS
DES MÉDECINS
VAUDOIS

Interview

“L’ensemble du cycle de vie des données doit être consigné”

Les professionnel-les de santé ont une responsabilité sociale toute particulière de par la sensibilité des données personnelles qu’ils et elles traitent quotidiennement. D’importants enjeux de santé publique en découlent. Les autorités sanitaires ont dès lors tout intérêt à veiller à l’intégration et au respect de normes sécuritaires strictes. DOC fait le point avec Adrian Lobsiger, Préposé fédéral à la protection des données et à la transparence (PFPDT).

Quel est le rôle de l’Etat cantonal/ fédéral face à la menace croissante de cyberattaques, particulièrement dans le domaine médical ?

Des enquêtes d’investigation menées sur les portails en ligne dans le domaine de la santé ainsi que les cyberattaques récentes contre des hôpitaux et cabinets médicaux suisses ont mis en évidence de graves lacunes en matière de sécurité et la nécessité d’agir dans ce domaine. Les autorités sanitaires ont leur responsabilité engagée lorsque des entreprises privées traitent des données de santé de leurs citoyen- nes. Ces actrices et acteurs privé-es soutenu-es par des fonds publics devraient appliquer des normes qui soient à la hauteur de celles que les autorités fédérales ou cantonales correspondantes s’appliquent à elles-mêmes. Nous attendons de ces dernières non seulement des concepts complets pour le traitement des données, mais aussi des tests de résistance externes. Concernant la sensibilisation aux cyberrisques, tant les autorités sanitaires que les actrices et acteurs privé-es du domaine de la santé (médecins, thérapeutes, hôpitaux) peuvent compter sur le soutien des autorités de protection des données de la Confédération et des cantons.

Qui porte la responsabilité de la protection des données médicales ?

La responsabilité d’une protection suffisante des données incombe aux personnes qui traitent ces données, c’est-àdire aux fournisseurs de prestations dans le domaine de la santé (hôpitaux, médecins, etc.). C’est donc à eux de mettre en place les garde-fous nécessaires pour éviter la multiplication de cyberattaques. Le PFPDT est chargé de veiller au respect des exigences minimales définies par la loi. Il peut conseiller les professionnel-les de la santé sur les questions de protection des données.

Comment les responsabilités sontelles réparties entre les échelons fédéraux et cantonaux et quelle collaboration entretenez-vous ?

Le PFPDT est responsable de la surveillance de la protection des données des autorités fédérales (par ex. l’Office fédéral de la santé publique) et des privés (notamment les cabinets médicaux et les pharmacies). Il remplit également une fonction de conseil. Les services de surveillance de la protection des données des cantons sont compétents pour la surveillance des établissements de santé cantonaux ou communaux (hôpitaux publics). En cas de questions relatives à la délimitation des compétences, les autorités de protection des données de la Confédération et des cantons s’entendent généralement directement et entretiennent en outre des échanges réguliers et fructueux sur des questions d’actualité dans le cadre de privatim, la Conférence des Préposé-es suisses à la protection des données.

> Les accès aux données relatives à la santé doivent être régulés de manière plus restrictive que les accès aux données administratives.

Quelles recommandations transmettre aux cabinets médicaux privés et aux hôpitaux pour se prémunir de ces attaques ?

Les exploitants d'hôpitaux publics ou privés ont besoin d'un personnel formé en conséquence qui, le cas échéant avec le concours de prestataires de services externes, veille entre autres à ce que les failles de sécurité connues soient comblées à temps par des mises à jour de logiciels. Les cabinets médicaux et thérapeutiques doivent également consacrer les moyens nécessaires à la sécurisation et à la mise à jour régulière des systèmes informatiques. Les collaborateurs/trices doivent être formé-es en conséquence. Si les connaissances font défaut à l'interne, il convient de faire appel à des spécialistes externes. Des accords sectoriels peuvent aider à contenir les coûts. Les actrices et acteurs mentionné-es doivent veiller à ce que des processus clairs et vérifiables soient mis en place pour le traitement et la conservation des données. L'ensemble du cycle de vie des données doit être consigné et les droits d'accès doivent être réglementés par catégorie : les accès aux données relatives à la santé doivent être régulés de manière plus restrictive que les accès aux données administratives. L'accès aux systèmes via des appareils non sécurisés – tels que les téléphones portables privés – doit être limité, les données doivent être cryptées et les mesures de sécurité doivent être réévaluées régulièrement. Pour éviter les interruptions critiques du système, il convient par ailleurs d'utiliser un système de sauvegarde et de restauration des données de haute qualité. Une copie des dossiers devrait enfin être faite régulièrement et conservée dans un endroit sûr : les données devraient être stockées localement, de préférence sur un disque dur externe, et tenues à jour. Afin de garantir la poursuite de l'activité, même en cas d'urgence, et de s'assurer que les données sont accessibles dans tous les cas et à tout moment, nous recommandons également de stocker les documents hors ligne.

Propos recueillis par la rédaction