DOC
LE RENDEZ-VOUS
DES MÉDECINS
VAUDOIS

Protection des données dans les cabinets médicaux

Que nous réserve la nouvelle législation dès 2023?

Dans un monde de plus en plus informatisé et malintentionné, il est essentiel d'avoir les bons réflexes pour éviter la perte et le vol de données, mais aussi pour maintenir sa réputation. Si le médecin et ses auxiliaires sont liés par le secret médical (art. 321 Code pénal), ils doivent également respecter la Loi sur la protection des données et leurs lois dites « métiers ».

Le médecin traite des données personnelles (identifiants, données administratives) et des données sensibles (données sur la santé, données génétiques) tout au long de sa carrière. Il les conserve soit sur papier, soit dans son système informatique (hébergé dans son cabinet ou chez un prestataire externe), ou les deux. Et surtout, le médecin les transmet à d'autres actrices et acteurs du domaine de la santé.

Avec l'entrée en vigueur de la nouvelle Loi sur la protection des données (nLPD) ainsi que son ordonnance (OPDo) le 1er septembre 2023, le médecin sera toujours considéré comme le responsable du traitement et est donc personnellement responsable en cas de fuite de données et de violation de la loi. Et les données sensibles bénéficient toujours d'une protection accrue. De plus, la nLPD renforce les droits des patient-es (personnes concernées) et accroît les obligations des médecins (responsables du traitement). Elle augmente également les sanctions pénales qui peuvent aller jusqu'à CHF 250'000.

Quelles obligations et quelle responsabilité pour le médecin en cabinet ?

La nLPD permet toujours le traitement (collecte, utilisation, enregistrement, etc.) de données – même sensibles – en respectant les principes généraux de protection des données : licéité (est-ce qu'une loi interdit le traitement des données ?) ; bonne foi ; finalité (quel est le but poursuivi ?) ; proportionnalité (est-ce que je ne collecte que ce qui est nécessaire au but poursuivi ?) ; reconnaissabilité (est-ce reconnaissable pour mon/ma patient-e ?) ; exactitude (les données collectées et conservées sont-elles exactes ?).

Le transfert des données sensibles à un tiers (assurances, pairs, laboratoires, établissements de santé, etc.) est possible, mais il doit se baser soit sur le consentement libre, éclairé et express du/de la patient-e, sur une base légale ou sur l'exécution de contrat de mandat du médecin avec son/sa patient-e (art. 30-31 nLPD). Le médecin doit donc s'assurer qu'il a un motif justificatif et le gérer, sachant que le consentement peut être retiré en tout temps.

Tout-e patient-e a le droit d'accéder à l'entier de son dossier (art. 25-26 nLPD – 24 LSP) sur simple demande, sans aucune raison, incluant les notes prises par le médecin contenant des indications nécessaires au traitement, mais pas celles rédigées exclusivement pour un usage personnel.

Bien que la Loi oblige les responsables du traitement à informer les personnes concernées lors du traitement de leurs données, le médecin est délié de ce devoir en raison du secret médical (art. 20 al. 1 lit c nLPD). Cependant, il doit s'assurer que le traitement est reconnaissable pour ses patient-es.

Dès que les données collectées ne sont plus nécessaires pour le but poursuivi, elles doivent être détruites ou anonymisées, à moins qu'une loi ne prévoie le contraire, comme la Loi sur la santé publique (LSP) qui requiert la conservation des dossiers pour une durée de 10 ans (art. 87) et 20 ans dans les cas visés par l'art. 128a du Code des obligations (mort d'homme, lésions corporelles).

Lors de son installation, le médecin devra s'assurer que le logiciel utilisé pour le traitement de ses dossiers prend en compte la protection des données (privacy by design) et que les questionnaires proposés à ses patient-es n'incluent que les données nécessaires pour prodiguer les soins et permettre la gestion administrative.

Enfin, la nouvelle Loi oblige les responsables du traitement à annoncer dans les meilleurs délais les cas de violation de la sécurité des données (hacking par exemple) auprès du Préposé fédéral à la protection des données et à la transparence (PFPDT), car il est certain qu'une fuite des données médicales engendre un risque élevé pour la personnalité des patient-es. Le médecin devra également informer ses patient-es.

Mesures organisationnelles et de sécurité

Le médecin devra mettre en place un registre des traitements dans lequel il indiquera l'identité du responsable du traitement (le médecin), la finalité du traitement (gestion administrative, soins médicaux), les personnes concernées (patient-es), le délai de conservation des dossiers médicaux (base légale si existante), les mesures de sécurité entreprises, à qui sont transférées les données (tiers, sous-traitants) et le nom de l'Etat concerné si les données sont transférées à l'étranger. En fonction de l'évolution de ses dossiers, le médecin devra mettre à jour son registre.

Le médecin devra avoir conclu des contrats avec ses sous-traitants (art. 9 nLPD) incluant des clauses de protection des données, notamment en cas d'hébergement informatique. Dans ce cas, il est conseillé de choisir un prestataire en Suisse, certifié ISO, ayant une capacité de restitution immédiate des données en cas de problèmes. Le médecin est responsable de s'assurer que les mesures de sécurité adéquates sont mises en place par le sous-traitant.

Que ce soit au cabinet ou en télétravail, des mesures de sécurité doivent être prises pour éviter la fuite de données, leur vol ou leur destruction. Le médecin doit notamment protéger les accès aux serveurs, garder les dossiers papiers sous clé (coffre-fort), faire des back-up (avec le même niveau de sécurité), surveiller et minimiser les accès aux données (imprimantes, écrans), instaurer des mots de passe, installer un économiseur d'écran à déclenchement immédiat, ne transférer que des données cryptées (lors de l'utilisation e-mail par exemple), installer des antivirus, éviter les accès Internet sur le même système ; et maintenir ses installations informatiques à jour (mises à jour). Une marche à suivre doit être prévue en cas de fuite de données et d'incidents de sécurité telle que la mise hors service des appareils ou encore le processus d'annonce au PFPDT.

Me Isabelle Hering
Avocate, médiatrice et DPO externe - Etude Hering, DPO Associates Sarl, Nyon