© FLY:D / Unsplash

La FMH aide ses membres à mettre en œuvre la nouvelle loi sur la protection des données.

LPD: des changements pour les cabinets médicaux

Protection des données La loi sur la protection des données (LPD), totalement révisée, entrera en vigueur le 1er septembre 2023. Elle contient de nombreuses nouveautés qui nécessitent diverses adaptations au niveau du traitement des données personnelles dans la pratique médicale. La FMH mettra à disposition des documents types à cet effet. Cet article présente les principales nouveautés et les différents outils à disposition.

Bruno Baeriswyl[a], Reinhold Sojer[b]
[a] Dr iur., conseiller à la protection des données de la FMH, [b] Dr rer. biol. hum., chef de la division Numérisation / eHealth de la FMH

Le but de la révision totale de la loi sur la protection des données (LPD) est comparable aux objectifs des réformes de la protection des données en Europe: le droit de la protection des données doit être adapté aux évolutions de la société numérique, afin de garantir les droits fondamentaux et les droits de la personnalité des citoyennes et citoyens. Les nouvelles dispositions visent à accroître la transparence en matière de traitement des données en concrétisant les conditions-cadres applicables à la gestion des données personnelles et en prévoyant une protection adéquate des données grâce à une technologie conçue à cet effet. Les principes en vue d'un traitement licite des données demeurent inchangés. Néanmoins, le maître du fichier ou le «responsable du traitement», comme il est appelé dans la nouvelle loi, doit respecter différentes nouvelles dispositions qui peuvent impliquer une adaptation des processus de traitement des données actuels.

Modèle de déclaration

Lors de la collecte de données personnelles, les personnes concernées doivent être informées de manière transparente concernant le traitement des données, en particulier la finalité du traitement et, le cas échéant, les destinataires auxquels les données sont transmises [1]. Cela implique dans de nombreux cas une modification de la déclaration de protection des données du cabinet médical. Quoi qu'il en soit, les déclarations de protection des données actuelles doivent être vérifiées au regard des nouvelles dispositions. La FMH mettra à disposition un modèle de déclaration de protection des données.

Dans la mesure où un consentement est requis pour le traitement de données sensibles, dont font partie les données relatives à la santé

d'une personne, ce consentement doit être exprès et n'est valable que si la personne concernée exprime librement sa volonté concernant un ou plusieurs traitements déterminés après avoir été dûment informée [2]. Le catalogue des données personnelles sensibles a été complété par les données génétiques et les données biométriques identifiant une personne physique de manière univoque [3]. La FMH met à disposition une déclaration de consentement qui permet de recueillir le consentement dans le cadre de l'information aux patientes et aux patients.

Un devoir d'informer existe également en cas de décision individuelle automatisée, par exemple lorsqu'une décision est prise par un algorithme, dans la mesure où celle-ci est prise exclusivement sur la base d'un traitement automatisé et affecte de manière significative la personne concernée [4]. S'agissant des diagnostics assistés par ordinateur, il faudra décider dans quelle mesure ceux-ci sont exclusivement automatisés et nécessitent donc une information correspondante des patientes et des patients.

La nouvelle loi sur la protection des données accorde une importance particulière à la conception technique et à la sécurité des données.

Technique et sécurité

L'actuel registre des fichiers devient un registre des activités de traitement [5]. L'obligation de tenir un tel registre ne s'applique certes plus à tous les responsables du traitement, mais elle est maintenue dès lors que «le traitement porte sur des données sensibles à grande échelle» [6]. Les cabinets médicaux et leurs dossiers de patientes et de patients sont donc régulièrement soumis à cette obligation. Le registre doit contenir les informations mentionnées de manière détaillée par la loi. Au moyen d'un modèle et d'un guide, la FMH met à disposition des cabinets médicaux la documentation nécessaire pour satisfaire aux exigences légales.

La nouvelle loi sur la protection des données accorde une importance particulière à la conception technique et à la sécurité des données. Le responsable du traitement est ainsi tenu de mettre en place des mesures techniques et organisationnelles afin que le traitement respecte les prescriptions de protection des données (privacy by design) [7]. Il est également tenu de garantir, par le biais de préréglages appropriés, que le traitement des données personnelles soit limité au minimum requis par la finalité poursuivie (privacy by default) [8]. De manière générale, le responsable du traitement doit garantir une sécurité des données personnelles adéquate par rapport au risque encouru [9] et s'assurer que tout sous-traitant auquel il fait recours soit en mesure de garantir la sécurité des données [10]. Les données relatives à la santé faisant partie des données sensibles, des mesures spécifiques sont nécessaires en matière de sécurité des données comme, par exemple, le recours à des technologies de chiffrement. En ce qui concerne la sécurité des données, la FMH adaptera les guides sur la sécurité informatique. Dans ce cadre, elle abordera également les nouvelles exigences concernant l'analyse d'impact relative à la protection des données [11] (analyse de risques) et l'élaboration d'un règlement sur le traitement des données [12] qui peut aussi documenter la licéité du traitement des données. Un concept de conservation et d'archivage devrait compléter le règlement de traitement. La FMH a élaboré un guide à ce sujet.

Dans certains cas, le cabinet médical doit annoncer une violation de la sécurité des données à l'autorité de surveillance, le Préposé fédéral à la protection des données et à la transparence (PFPDT) [13]. Il y a violation de la sécurité des données par exemple lorsqu'une clé USB contenant des données personnelles est perdue ou que le système du cabinet a été «piraté» de l'extérieur. L'obligation d'annoncer n'existe que si la violation entraîne vraisemblablement un risque élevé pour la personnalité de la personne concernée, ce qui ne peut pas être exclu d'emblée s'agissant de données relatives à la santé. Il est donc recommandé aux cabinets médicaux de définir une procédure pour faire face à de telles situations. La FMH met à disposition à cet effet une check-list et une description de la procédure à suivre en cas de violations de la protection des données.

Comme jusqu'à présent, les personnes concernées doivent être informées des données traitées les concernant.

Droit d'accès

Comme jusqu'à présent, les personnes concernées doivent être informées des données traitées les concernant (droit d'accès) [14]. Demeure également valable la règle selon laquelle des données peuvent être communiquées aux personnes concernées, moyennant leur consentement, par l'intermédiaire d'un professionnel de la santé qu'elles auront désigné. Le droit d'accès implique le droit d'obtenir des copies du dossier de la patiente ou du patient mais pas, en principe, le droit à la remise du dossier médical. Afin que les demandes de renseignements ou de remise soient traitées de manière correcte, la FMH a remanié les instructions existantes.

La nouvelle loi sur la protection des données contient de nombreuses dispositions pénales [15]. Celles-ci sanctionnent en particulier la violation des obligations d'informer, de renseigner et de collaborer ainsi que la violation des devoirs de diligence. La loi prévoit des amendes allant jusqu'à 250 000 francs. Seules sont punissables, sur plainte, les personnes qui contreviennent intentionnellement à ces obligations, c'est-à-dire qu'elles agissent avec conscience et volonté. Si les données sont traitées de manière responsable, ce à quoi servent les outils de la FMH, ces conditions de punissabilité ne risquent guère d'être remplies. Comme jusqu'à présent, le secret professionnel (art. 321 du Code pénal suisse) reste essentiel; il doit également être respecté dans le cadre d'un traitement de données toujours plus numérisé. Il est important à cet égard que cette obligation de garder le secret soit également imposée aux collaboratrices et collaborateurs ou aux tiers externes agissant en qualité d'auxiliaires. Il existe pour les deux cas de figure des déclarations de confidentialité de la FMH.

Outils élaborés par la FMH en relation avec la nouvelle loi sur la protection des données (LPD)

- Déclaration de protection des données
- Déclaration de consentement
- Modèle et guide pour le registre des activités de traitement
- Guide pour la conservation et l'archivage
- Check-list et déroulement de la procédure en cas de violations de la protection des données
- Instructions relatives aux demandes de renseignements et de remise
- Déclarations de confidentialité

Correspondance
ehealth[at]fmh.ch

Références
Liste complète des références sous www.bullmed.ch ou via code QR