RGPD, cyber et autres: points importants pour les médecins*

Liliane Mollet

Juriste et conseillère à la protection des données de la FMH

Les médecins reçoivent chaque jour des informations extrêmement sensibles et intimes sur leurs patients. Ils assument donc une grande responsabilité en matière de protection et de sécurité des données. Appartenant à la catégorie «données sensibles», ces informations personnelles sont protégées par la loi fédérale sur la protection des données. Le règlement général sur la protection des données de l'Union européenne en vigueur depuis le 25 mai 2018 pose des exigences supplémentaires qui peuvent concerner les médecins. En voici l'essentiel.

RGPD: de quoi s'agit-il?

Par son nouveau règlement général sur la protection des données (RGPD), l'Union européenne s'est dotée d'un ensemble complet de dispositions visant la protection des données à caractère personnel. Les principaux éléments déclencheurs ont été, d'une part, la mise en réseau rapide et la numérisation progressive de toutes les sphères de la vie et, d'autre part, les différences dans le niveau de protection d'un Etat à l'autre de l'UE, qui faussent la concurrence. Aujourd'hui, de grandes quantités de données personnelles sont recueillies, associées et traitées pour fournir de nouvelles informations. Pour des personnes physiques comme les médecins et les patients, il devient de plus en plus difficile de savoir quelles données sont enregistrées à quel endroit, qui peut y accéder et comment elles sont traitées. Cela entraîne une réduction de l'autodétermination de ces personnes en matière d'information, c'est-à-dire de leur liberté de décider si et comment les données les concernant peuvent être utilisées. En outre, elles ne sont plus vraiment en mesure de faire valoir leurs droits légaux en raison du manque de transparence dans la gestion de leurs données personnelles (p. ex. le droit d'accéder aux données ou de prendre part aux décisions, lorsque celles-ci sont prises par des logiciels). Il faut leur redonner la possibilité de mieux contrôler les données les concernant. C'est pourquoi la législation sur la protection des données a fait l'objet d'une révision globale au niveau européen, y compris en Suisse. La «directive Schengen» et la «Convention du Conseil de l'Europe 108» ont déjà été remaniées. Ces deux accords internationaux étant contraignants pour la Suisse, celle-ci est obligée d'adapter sa propre loi sur la protection des données (LPD). Le contenu de ces accords s'aligne dans une large mesure sur le RGPD et il faudrait éviter que l'économie suisse fasse les frais de divergences entre les réglementations, si bien que la future loi fédérale s'inspirera du RGPD. Les entreprises suisses, qui appliquent déjà le RGPD, seront aussi prêtes pour la nouvelle LPD.

Droit européen pour les cabinets et hôpitaux de Suisse?

Le RGPD ne s'applique en principe qu'à l'UE (et aux membres de l'EEE depuis le 20 juillet 2018). Etant donné que la Suisse n'est ni membre de l'UE, ni membre de l'EEE, elle est considérée comme Etat tiers dans le cadre du RGPD. Cela signifie que les entreprises suisses restent soumises à la loi fédérale sur la protection des données. Cependant, le RGPD a prévu des cas dans lesquels le contact avec l'UE est si fort que l'application de ce règlement se justifie aussi pour les Etats tiers. Tel est notamment le cas lorsque des cabinets médicaux ou des hôpitaux adressent clairement leurs prestations à des patients établis dans l'UE. Il en va de même pour les cabinets ou les hôpitaux possédant un établissement sur le territoire de l'UE. Le RGPD est également applicable lorsque le comportement d'internautes établis dans l'UE est «surveillé», par exemple, via le site Internet d'un cabinet ou d'un hôpital. Cela peut notamment se faire à l'aide de cookies ou d'outils d'analyse tels que Google Analytics. Il faudra cependant tenir compte de la situation concrète du cabinet ou de l'hôpital.

* Cet article est déjà paru dans la revue Synapse (Mollet L. DSGVO, Cyber & Co.: Was müssen Ärztinnen und Ärzte beachten? Synapse. 2018;4:5–7).

Quels sont les changements apportés par la nouvelle législation?

Le RGPD n'est pas quelque chose d'entièrement nouveau. Un grand nombre des principes et des droits qu'il contient figurent déjà dans la loi fédérale sur la protection des données (les principes de proportionnalité et de minimisation, p. ex.). Des dispositions légales réglaient déjà les modalités ainsi que la finalité de la collecte et du traitement des données avant le RGPD. Celui-ci renforce cependant certaines règles et contraint les responsables (personne physique ou organisation traitant des données personnelles) à documenter les données collectées de façon transparente et compréhensible. En outre, il prévoit des sanctions sévères en cas de violation des nouvelles dispositions sur la protection des données. Cela vaut aussi pour le quotidien des médecins en Suisse: si en principe pas grand-chose ne change pour le traitement des données personnelles, les médecins devront fournir à l'avenir des informations plus concrètes, documenter davantage les traitements de données personnelles effectués et prouver la conformité de ceux-ci aux dispositions légales. Toutes les personnes physiques dont les données sont traitées devront donc en être informées (au moyen d'un contrat, d'une mention sur le formulaire d'inscription du patient ou d'une déclaration de confidentialité sur le site Internet, p. ex.).

Quels sont les aspects importants pour les médecins?

Indépendamment de l'applicabilité du RGPD, il vaut la peine de passer en revue certains points concernant le traitement des données de patients, en s'appuyant sur les exigences et les principes de ce règlement.

1. Analyse de la situation

Le point de départ doit toujours être une vue d'ensemble des données, des systèmes et des interactions. Des questions et des réponses simples, d'ordre général, permettent d'obtenir rapidement un premier aperçu de la situation du cabinet ou de l'hôpital: le RGPD est-il applicable? Où le cabinet / l'hôpital est-il situé? A qui s'adressent les prestations? Nombre d'employés internes et externes? Nombre moyen de patients? Nombre de postes de travail, d'applications et de serveurs connectés à Internet? Où se trouvent les données sur les patients (dans le cabinet ou l'hôpital, dans un cloud ou sur papier)? Ces quelques points donnent déjà une idée de la situation. En outre, ils constituent une base importante pour l'évaluation individuelle des risques.

2. Approche fondée sur les risques: fixer des priorités

Le niveau des mesures de protection des données à mettre en œuvre dépend de l'estimation de la situation personnelle (emplacement central ou périphérique, transferts réguliers de données dans des Etats tiers peu sûrs, processus numériques de grande ampleur avec des données de patients délicates ou des applications peu transparentes, p. ex.) et de l'appétence pour le risque. Lorsque le risque est élevé pour les patients concernés, il est parfois nécessaire de mener une analyse d'impact relative à la protection des données (une sorte d'analyse du risque par rapport au traitement concret des données et aux conséquences possibles sur les personnes concernées) pour un processus précis ou une application. Les thèmes critiques tels que les données et les droits des patients ainsi que les données sur le personnel doivent être prioritaires. Le site Internet et la visibilité vis-à-vis de l'extérieur sont également très importants, car il s'agit généralement du premier point de contact pour les patients et pour les autorités de surveillance de la protection des données. De plus, un cabinet ou un hôpital peut justement se servir de son site Internet pour prouver que les exigences de la protection des données sont respectées et pour montrer sa compétence en la matière. Ainsi, un site Internet peut déjà contribuer considérablement à l'obligation d'informer et permet d'attirer l'attention sur les droits des personnes concernées (le droit d'accès, p. ex.). Il ne remplace cependant pas l'information concrète aux patients (voir ce qui suit).

3. Registre des activités critiques de traitement des données («Data Mapping»)

Chaque cabinet ou hôpital doit tenir un registre des activités de traitement des données effectuées sous sa responsabilité. Peu importe la forme sous laquelle les données personnelles sont présentées (données électroniques, liste sur papier ou radiographies, p. ex.), le registre doit contenir les informations minimales requises par la loi (le nom et les coordonnées de la personne responsable, la nature des données, la finalité du traitement des données et les destinataires des données, p. ex.). La base légale sur laquelle repose le traitement des données concerné (consentement du patient, exécution d'un contrat, intérêt légitime du médecin, p. ex.) ainsi que les mesures organisationnelles et techniques mises en œuvre pour protéger les données personnelles sont des informations supplémentaires utiles. Ce registre sert en même temps à prouver que les exigences légales ont été respectées (obligation d'établir une documentation, principe de responsabilité, p. ex.). On trouve différents modèles de registres sur Internet (voir sous «Liens» à la fin de cet article).

4. Directives internes relatives à la protection des données

Les directives internes relatives à la protection des données sont un ensemble de règles régissant le traitement des données personnelles. Elles contiennent des dispositions contraignantes et centrales sur la gestion des données personnelles au sein du cabinet ou de l'hôpital. Tous les collaborateurs du cabinet ou de l'hôpital sont tenus de suivre ce règlement interne. De telles directives apportent davantage de clarté et jettent les bases pour une compréhension commune et une gestion uniforme des données personnelles. Elles doivent au minimum inclure les principes de la protection des données en vigueur en Suisse (voir la vue d'ensemble de ces principes dans l'annexe des directives de 2014 sur les exigences minimales qu'un système de gestion de la protection des données doit remplir, qui est utilisée dans le cadre des certifications en matière de protection des données). D'autres éléments importants sont, entre autres, des responsabilités clairement définies, des règles pour la gestion des données de patients et les procédures mises en place pour l'exercice des droits des personnes concernées (droit d'accès, p. ex.).

5. Personnel: rapports et contrats de travail

L'ensemble des collaborateurs du cabinet ou de l'hôpital devraient s'engager par écrit à respecter la confidentialité des données et à observer les directives relatives à la protection des données. Combinée à une sensibilisation et à une formation régulière dans le domaine de la protection et de la sécurité des données, cette obligation contribue fortement à la protection des données personnelles.

On peut se demander si le RGPD est applicable aux rapports de travail des citoyens de l'UE qui travaillent dans un cabinet en tant que frontaliers. La réponse est négative, car le RGPD se rapporte à l'offre de biens ou de services depuis la Suisse vers l'UE. Or, l'employeur n'offre ni biens ni services dans le sens de l'art. 3 al. 2 let. a RGPD dans l'Union européenne. En outre, les citoyens de l'UE se trouvent en Suisse au moment où ils fournissent leur prestation de travail et traitent les données. La demande de prestations de travail dans l'UE ainsi que les rapports de travail en Suisse ne sont donc pas soumis au RGPD.

6. Patientes et patients: droits des personnes concernées

Les données personnelles telles que les données de patients ne peuvent être traitées que si une base légale spécifique le permet. Conformément à la loi, les données de patients sont sensibles et, comme mentionné plus haut, doivent être traitées avec un soin particulier. De plus, les patients peuvent à tout moment faire valoir leurs droits légaux à la protection des données envers leur médecin.

a) Consentement

Les soins aux patients sont basés sur le contrat thérapeutique passé entre le médecin et le patient. Les conditions de ce contrat découlent essentiellement du droit cantonal relatif à la santé et aux hôpitaux. Pour le traitement des données de patients, il faut en plus un consentement exprès du patient, vu qu'il s'agit de données sensibles. Le médecin ou l'hôpital doit pouvoir prouver que la personne concernée a donné son accord au traitement des données le concernant dans le but mentionné explicitement (= de manière active) et de son plein gré (= sans contrainte). C'est aussi le cas lorsque des données personnelles sont transmises à des tiers (caisses de médecins ou sociétés de recouvrement, p. ex.) ou destinées à être traitées à d'autres fins (recherche médicale, p. ex.). En outre, la demande de consentement doit être présentée «sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples». Il faut aussi que ce consentement puisse être distingué clairement des autres questions. Notons encore qu'il peut être retiré à tout moment (droit de retrait).

b) Obligation d'informer

Le RGPD fixe des exigences accrues concernant le devoir d'informer. Les médecins sont tenus d'informer activement leurs patients sur la collecte et la conservation de données personnelles. Cette information doit être communiquée «d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples». Les points suivants doivent absolument être communiqués: l'identité et les coordonnées du responsable du traitement, les finalités du traitement auquel les données sont destinées, les bases légales du traitement et, le cas échéant, les destinataires des données. Si les données personnelles n'ont pas été collectées auprès de la personne concernée (le patient), il faut en plus communiquer la nature des données. L'obligation d'informer peut par exemple être remplie au moyen d'une information sur le site Internet du cabinet ou de l'hôpital, sur des affiches dans la salle d'attente ou sur le formulaire d'inscription du patient.

c) Droit d'accès

Tout patient a le droit de savoir quelles données le concernant sont enregistrées et conservées. Ce droit existe depuis longtemps dans la loi fédérale sur la protection des données. La personne concernée peut en faire usage pour faire valoir ses droits à la protection

des données ainsi que son droit à la portabilité ou à l'effacement des données, afin de garder le contrôle des données collectées à son sujet. Elle doit présenter elle-même sa demande au médecin.

d) Droit à l'effacement
Les données personnelles et les données de patients ne peuvent pas être conservées et/ou archivées de manière illimitée («droit à l'oubli»). Il convient d'observer les délais légaux fixés pour la conservation et l'effacement. La directive interne sur la protection des données précitée est un bon instrument pour fixer de tels délais et processus. Les médecins doivent être conscients que le droit à l'effacement ne s'applique pas à tous les cas et qu'il existe certains délais légaux de conservation.

7. Prestataires externes et tiers

Il est conseillé de vérifier si les contrats passés avec des prestataires externes (services informatiques ou caisses de médecins, p. ex.) sont compatibles avec les nouvelles exigences du RGPD, tout en tenant compte de la révision en cours de la loi fédérale sur la protection des données en Suisse.
Dès que des données de patients font l'objet d'un traitement électronique ou sont traitées dans une application, des sous-traitants, par exemple des fournisseurs de services informatiques, sont généralement chargés de la maintenance de ces systèmes. Il peut arriver que des informaticiens externes aient accès au logiciel du cabinet et puissent même consulter les données des patients. Le RGPD précise les conditions devant désormais être réglées avec les sous-traitants pour assurer la protection des données (annexées au contrat d'assistance et de maintenance existant). Les sous-traitants et leurs collaborateurs doivent notamment s'engager par écrit à respecter le secret professionnel. Les prestataires de services informatiques d'une certaine importance ont déjà établi des avenants au contrat ou des conventions à signer qui tiennent compte du RGPD.

8. Sécurité des données et cybersécurité

La cybercriminalité, notamment le piratage des réseaux des hôpitaux ou la vente de données de patients sur le «darknet», est un sujet très actuel. Le risque que des données de patients soient utilisées frauduleusement à des fins criminelles telles que le vol d'identité ou l'hameçonnage («phishing») ne cesse d'augmenter. La numérisation progressive accentue encore cette situation. Une sécurité à 100% ne sera jamais possible. Il ne faut pas abandonner, mais se concentrer sur la protection de base des ordinateurs et des appareils mobiles, les tester régulièrement et les optimiser (une fois de plus: approche basée sur le risque). Rappelons que le plus gros risque pour la sécurité reste l'humain et le personnel interne ou externe, et non la technique! De ce fait, une sécurité à plusieurs niveaux doit être assurée: des mesures organisationnelles (sensibilisations et formations régulières surtout) combinées à des mesures techniques (pare-feux personnels actuels installés sur tous les appareils, mises à jour régulières de tous les logiciels, p. ex.) constituent la protection la plus efficace. Pour cela aussi, il existe des aides sur Internet (voir «Liens» ci-dessous). Ces mesures devraient correspondre à l'évaluation individuelle des risques. Finalement, les mesures prises par le cabinet médical ou l'hôpital doivent être documentées et doivent pouvoir être démontrées.

Liens

- PFPDT – La protection des données au cabinet médical: https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/gesundheit/la-protection-des-donnees-au-cabinet-medical.html
- CNIL – Guide de la sécurité des données personnelles: https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles
- CNIL – voir sous «Je suis un particulier»: recommandations et check-lists utiles pour la sécurité dans les cabinets médicaux et à la maison https://www.cnil.fr/
- Ordre National des Médecins et CNIL – Guide pratique sur la protection des données personnelles: https://www.conseil-national.medecin.fr/sites/default/files/guide_cnom_cnil_rgpd.pdf

Correspondance:
FMH
Préposée à la protection des données
Elfenstrasse 18
Case postale 300
CH-3000 Berne 15
datenschutz[at]fmh.ch