Fiche d'information sur la protection des données dans les cabinets médicaux (site internet de la FMH)

Version 03/2023

La loi fédérale sur la protection des données et son ordonnance ont pour but de protéger la personnalité et les droits fondamentaux des personnes physiques dont les données personnelles sont traitées. Les médecins et leur personnel doivent traiter les données personnelles conformément à ces exigences légales.

La présente fiche d'information explique en quoi consiste la protection des données, ce que cela implique pour les cabinets médicaux et ce dont il faut tenir compte dans ce contexte. Des liens vers des outils tels que des modèles, des processus ou des listes de contrôle ont été insérés dans les différents chapitres, dans le but de soutenir les cabinets médicaux dans leur gestion de la protection des données. En plus du présent document, il est possible de consulter une FAQ sur le thème de la protection des données dans les cabinets médicaux.

But et finalité de la protection des données

La protection des données porte sur l'autodétermination en matière d'information et la protection contre les traitements abusifs de données portant atteinte à la personnalité ou aux droits fondamentaux des personnes physiques.

La loi sur la protection des données a pour but de protéger ces droits en définissant des prescriptions relatives à la gestion et au traitement des données personnelles.

Modifications apportées par la nouvelle loi sur la protection des données

La loi sur la protection des données (LPD) révisée, qui entrera en vigueur le 1er septembre 2023, renforce en particulier l'autodétermination des personnes concernées quant à leurs propres données en imposant aux responsables du traitement une transparence accrue et en étendant les droits des personnes concernées. Pour les cabinets médicaux, les principales modifications sont les suivantes :

— La définition des données sensibles est étendue aux données génétiques et biométriques, pour autant qu'elles permettent d'identifier une personne physique de manière univoque. Les conditions plus strictes du traitement de données sensibles s'appliqueront à l'avenir également à ces types de données.
— L'actuel registre des fichiers est remplacé par un registre des activités de traitement.
Ainsi, l'accent n'est plus mis sur les fichiers, mais sur la manière dont sont traitées les données personnelles ainsi que la finalité de ce traitement (cf. section « Tenue du registre des activités de traitement »).
— La loi prévoit désormais la réalisation d'une analyse d'impact relative à la protection des données (AIPD) lorsque le traitement envisagé est susceptible d'entraîner un risque élevé pour les droits de la personnalité ou les droits fondamentaux de la personne concernée. Un tel risque peut par exemple survenir lors du traitement de données sensibles telles que des données sur la santé ou en cas de recours à des nouvelles technologies (p. ex. produits cloud, intelligence artificielle) dans le cadre du traitement de données personnelles. Il est possible de renoncer à une analyse d'impact lorsque le traitement est effectué en vertu d'une

obligation légale, lorsque les systèmes, produits ou services utilisés pour le traitement envisagé sont certifiés ou qu'il est prévu de respecter un code de conduite soumis au Préposé fédéral à la protection des données et à la transparence (PFPDT).
— La loi révisée prévoit une obligation d'annoncer les violations de la sécurité des données (cf. section « Obligation d'annoncer les violations de la sécurité des données »).
— Les dispositions pénales de la LPD sont renforcées (cf. section « Dispositions pénales en matière de protection des données »)

Données personnelles

Par données personnelles ou données à caractère personnel, on entend toutes les informations concernant une personne, qui permettent de l'identifier ou de contribuer à l'identifier.
La notion de données personnelles doit donc être comprise au sens large.

La loi sur la protection des données distingue alors les données personnelles des données sensibles. Toutes les données personnelles sont en principe dignes de protection. La loi prévoit toutefois des exigences supplémentaires pour le traitement de données sensibles. La loi désigne notamment comme données sensibles les données sur la santé, la sphère intime, les opinions ou les activités religieuses, philosophiques, politiques ou syndicales.

Font par exemple partie des données personnelles traitées dans les cabinets médicaux :
— les données de base et les coordonnées de la patientèle, du personnel, des personnes de contact des prestataires de services ou d'autres établissements de santé (p. ex. nom, numéro de téléphone, adresse, adresse e-mail ou date de naissance) ;
— les saisies et enregistrements relatifs au déroulement d'un traitement, à la description des symptômes, aux diagnostics, aux ordonnances, aux réactions, aux résultats de laboratoire, aux radiographies, aux médicaments ;
— le statut d'assurances sociales ;
— les données relatives à la sphère intime, telles que l'état de santé, la vie sexuelle ou affective ;
— les données relatives au personnel et aux rapports de travail, y compris les évaluations des performances et les décomptes de salaires

Principes du traitement

Le traitement au sens de la LPD comprend toute opération relative à des données personnelles, quels que soient les moyens et les procédés utilisés, notamment la collecte, la conservation, l'utilisation, la modification, la communication, l'archivage ou la destruction des données. Les principes suivants s'appliquent au traitement de données personnelles :

— Le traitement de données personnelles est en principe licite lorsque l'ordre juridique en vigueur et les prescriptions en matière de protection des données sont respectés.
— Dans le cadre du traitement de données personnelles, les médecins ont un devoir d'information à l'égard des personnes concernées (notamment de la patientèle). Les médecins sont tenus d'informer leur patientèle de manière compréhensible sur le traitement des données, sur la finalité de la collecte et du traitement des données ainsi que sur les catégories de destinataires auxquels les données sont transmises.

— Afin d'assurer une information suffisante de la patientèle, les médecins utilisent des formulaires d'information, signés par la patiente ou le patient à l'issue des entretiens d'information, confirmant ainsi avoir compris les informations fournies et consentir à l'étape du traitement concerné.
— La collecte et la finalité du traitement doivent être effectuées de manière transparente et conforme au principe de la bonne foi. S'il n'est pas visible pour la personne concernée que des données sont collectées et / ou que la finalité du traitement n'est pas claire, elle doit en être informée. Le principe de la bonne foi signifie également que les données ne sont traitées que dans l'étendue à laquelle la personne concernée peut s'attendre.

Dans un souci de transparence, les cabinets médicaux peuvent par exemple mettre à disposition une déclaration de consentement ou une déclaration de protection des données, donnant des informations sur le traitement des données.

— Le traitement des données personnelles doit être proportionné. La proportionnalité est assurée lorsque le traitement est limité aux données appropriées et nécessaires à l'accomplissement de la tâche ou à l'atteinte de la finalité indiquée. La proportionnalité signifie en outre que la durée de conservation des données personnelles ne doit pas dépasser le temps pendant lequel elles sont effectivement nécessaires à l'accomplissement de la tâche ou la durée requise par une obligation légale de conservation (20 ans dès le départ du patient). Si des données personnelles ne sont plus nécessaires et qu'aucune obligation légale de conservation ne s'oppose à leur effacement, elles doivent être effacées définitivement.

— Le traitement doit être approprié. Il l'est lorsque le traitement des données personnelles n'est effectué que pour la finalité définie et indiquée lors de la collecte des données.
— Si les données personnelles sont erronées, elles doivent être rectifiées ou effacées.

Par exemple si la patiente ou le patient déménage ou change de caisse-maladie.

<u>Responsabilité au sein du cabinet médical</u>
La personne responsable du traitement au sens de la loi sur la protection des données est en principe le cabinet médical. Il est responsable du respect de la protection des données et doit en particulier veiller à la protection des droits de la personnalité et des droits fondamentaux de sa patientèle ainsi que de son personnel.
Si un cabinet médical souhaite de l'aide dans la mise en œuvre des exigences en matière de protection des données ou s'il en a besoin, il peut faire appel à une conseillère ou un conseiller à la protection des données interne ou externe. Le recours à des tels conseils est facultatif pour les cabinets médicaux relevant du droit privé et ne constitue pas une obligation légale.

La conseillère ou le conseiller à la protection des données est l'interlocuteur des personnes concernées pour toute question en la matière ainsi que celui du PFPDT ou des autorités cantonales chargées de la protection des données. Ses tâches sont de soutenir, conseiller et former le personnel de l'entreprise concernée en matière de protection des données ainsi que de participer à la mise en œuvre des exigences en la matière (p. ex. lors du traitement des demandes des personnes concernées [devoir d'information, droit d'accès, remise des données, etc.], lors de l'élaboration de règles internes en matière de protection des données, etc.).

Sécurité des données

Les données personnelles doivent être protégées contre les accès non autorisés, les modifications et les pertes afin de garantir la protection des droits de la personnalité et des droits fondamentaux de la patientèle et du personnel. Le cabinet médical doit prendre des mesures techniques et organisationnelles appropriées en matière de sécurité des données. Le choix de telles mesures dépend en principe du risque encouru. Il convient par conséquent de respecter les prescriptions relatives à la sécurité des données de l'ordonnance relative à la loi fédérale sur la protection des données (OPD) révisée.

Les restrictions d'accès aux systèmes et aux données physiques (p. ex. dossiers papier), la sauvegarde des données (backups), la formation du personnel, etc. constituent des exemples de mesures techniques et organisationnelles.

Obligation d'annoncer les violations de la sécurité des données

Il y a violation de la sécurité des données lorsque la confidentialité, l'intégrité ou la disponibilité des données personnelles est violée. Tel est par exemple le cas lorsque des données sont

— perdues ;
— effacées, détruites ou modifiées accidentellement ou sans autorisation ; ou
— accessibles à des personnes non autorisées ou consultables par elles.

Une violation de la sécurité des données pourrait par exemple être causée par :

— une erreur humaine ;
— des actes criminels (hacking) ;
— des malwares (introduction de logiciels malveillants) ;
— la perte ou le vol d'appareils (p. ex. ordinateurs portables), de supports de données (p. ex. clés USB, disques durs, CD / DVD) ou de documents papier.

Tout cas de violation de la sécurité des données entraînant un risque élevé pour les droits de la personnalité ou les droits fondamentaux des personnes concernées doit être annoncé dans les meilleurs délais au PFPDT, conformément à la loi fédérale révisée sur la protection des données et à son ordonnance. Lorsque la violation de la sécurité des données n'a pas de conséquences pour la personne concernée ou seulement des conséquences minimes, il est possible de renoncer à l'annoncer.

L'annonce contient au moins les indications suivantes :

— la nature de la violation de la sécurité des données (p. ex. destruction des données, vol des données, etc.) ;
— la date et la durée de la violation, lorsqu'elles sont connues ;
— les catégories de données personnelles et le nombre approximatif de données personnelles concernées, dans la mesure du possible ;
— les catégories de personnes concernées et le nombre approximatif de personnes concernées, dans la mesure du possible ;
— les conséquences de la violation de la sécurité des données, y compris les éventuels risques pour les personnes concernées (p. ex. impossibilité d'accès aux dossiers médicaux ne permettant qu'une traçabilité partielle du traitement, ce qui engendre un risque potentiel

pour la santé de la personne concernée ; publication des dossiers médicaux sur le darknet, ce qui met en danger la personnalité de la personne concernée) ;
— les mesures prises ou envisagées pour remédier au défaut ou en atténuer les conséquences (p. ex. restauration de la sauvegarde de données numériques) ;
— le nom et les coordonnées d'une personne de contact.

S'il n'est pas possible de communiquer toutes les informations en même temps, les informations restantes peuvent être mises à la disposition du PFPDT petit à petit, dans un délai raisonnable.

Droit d'accès des personnes concernées

Les patientes et les patients ont le droit d'obtenir gratuitement des renseignements sur les données les concernant et leur traitement, sans indication de motifs, pour autant qu'il n'existe aucune raison justifiant de refuser, restreindre ou différer un renseignement. La personne requérante doit pouvoir savoir dans un délai de 30 jours si des données la concernant sont traitées et, le cas échéant, de quelle manière.

Tenue du registre des activités de traitement

La personne responsable du traitement qui procède à un traitement important de données sensibles (p. ex. des données relatives à la santé) ou à un profilage à risque élevé doit tenir un registre des activités de traitement. En raison de la sensibilité des données sur la santé, il est recommandé aux médecins et aux cabinets de tenir au moins un registre des activités de traitement centrées sur le traitement de données sensibles (p. ex. tenue et gestion des dossiers médicaux, gestion des données de la patientèle relatives au décompte des assurances sociales, etc.).

Le registre doit contenir au moins les indications suivantes :
— la fonction ou personne responsable du traitement ;
— la description du traitement et de sa finalité ;
— les catégories de données personnelles traitées ;
— les catégories de personnes concernées ;
— les catégories de destinataires dès lors que des données sont régulièrement communiquées à des tiers ;
— les États vers lesquels les données sont éventuellement transférées ainsi que les garanties existantes, pour les États tiers dont la législation n'assure pas une protection des données adéquate ;
— le délai de conservation des données ou les critères pour déterminer cette durée si celle-ci n'est pas connue ;
— une description des mesures techniques et organisationnelles visant à garantir la sécurité des données ;
— l'origine des données, dès lors qu'elles n'ont pas été collectées auprès de la personne concernée

Sous-traitance

L'article de la loi révisée sur la protection des données réglemente le traitement des données par un sous-traitant. On parle par exemple de sous-traitance lorsqu'un système informatique

est externalisé vers un centre de calcul externe ou que le décompte des salaires et des honoraires est externalisé.

Dispositions pénales en matière de protection des données

En vertu de la loi sur la protection des données révisée, la violation d'exigences impératives en matière de protection des données peut, dans certains cas, entraîner une punissabilité personnelle. La personne physique fautive est alors punie d'une amende de 250'000 francs au plus, à condition que la violation de la protection des données ait été commise intentionnellement, c'est-à-dire que les obligations de coopération et de diligence aient été violées consciemment et volontairement.

Villars-sur-Glâne, le 21 septembre 2023