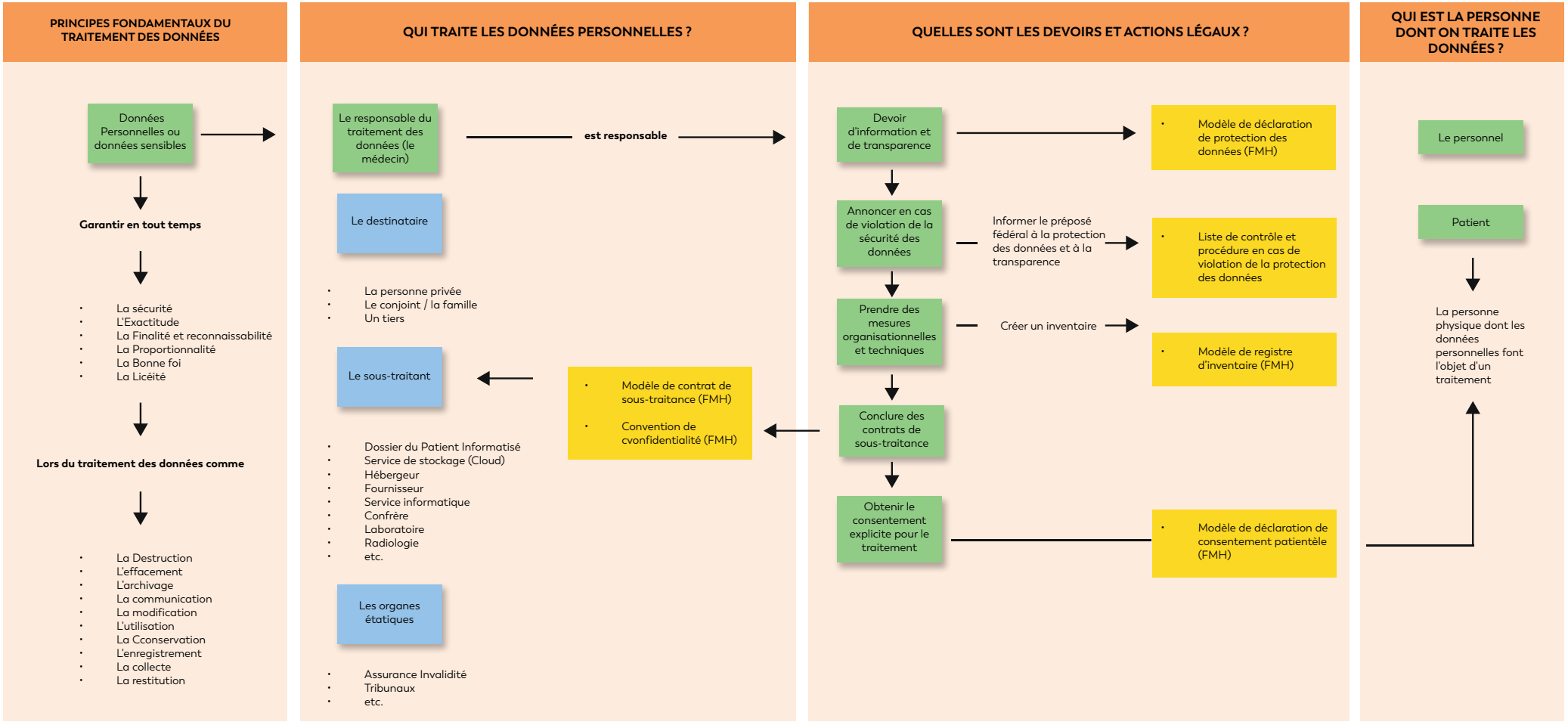
SOCIÉTÉ VAUDOISE DE MÉDECINE

Loi sur la Protection des Données

UN SCHÉMA SIMPLIFIÉ

Mise en oeuvre des principes fondamentaux et obligations principales pour les médecins et les cabinets médicaux: www.svmed.ch/lpd



Société Vaudoise de Médecine
Chemin de Mornex 38
1003 Lausanne

021 651 05 05
info@svmed.ch
www.svmed.ch

Nous restons à votre disposition pour répondre à vos questions.
Votre SVM - 21.08.2023

Obligations principales du responsable du traitement - www.svmed.ch/lpd

1. Le devoir d'information et de transparence

- Les médecins et les cabinets médicaux doivent informer la patientèle de manière transparente sur le traitement des données, en particulier la finalité du traitement et, le cas échéant, les destinataires auxquels les données sont transmises.
- Afin de respecter cette obligation, les médecins mettent à disposition un document intitulé «déclaration de protection des données». Pour les médecins et les cabinets médicaux qui en possèdent déjà, il faut vérifier que celui-ci est à jour et conforme avec la nLPD. Un modèle de déclaration de protection des données est mis à disposition par la FMH.
- Le lien vers ce document peut figurer sur les pieds de page des sites web des cabinets médicaux, dans les signatures des courriels, etc.

2. Le devoir d'obtenir le consentement explicite pour le traitement des données sensibles

- Le traitement des données sensibles (dont font partie les données relatives à la santé d'une personne) nécessite le consentement explicite de la personne concernée (art. 6 al. 7 nLPD). En effet, le consentement n'est valable que si la personne concernée exprime librement sa volonté concernant un ou plusieurs traitements déterminés après avoir été dûment informée (art. 30 al. 2 nLPD) .
- Afin d'assurer une information suffisante de la patientèle et obtenir un consentement libre et éclairé, les médecins et les cabinets médicaux utilisent des formulaires d'information (appelés encore déclaration de consentement/formulaire patientèle), 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.
- Un modèle de déclaration de consentement, formulaire patientèle est mis à disposition par la FMH. Il permet de recueillir le consentement du patient et l'informer sur le traitement de ses données.

3. Le devoir de conclure des contrats de sous-traitance dans le cadre de traitement de données par les tiers

- La loi impose des contrats de sous-traitance dans le cadre du traitement des données médicales par des tiers. De plus, les données médicales doivent être traitées de manière confidentielle.
- Les médecins et les cabinets médicaux doivent faire signer des contrats de sous-traitance et des conventions de confidentialité à leurs sous-traitants. Certains sous-traitants viendront certainement vers les médecins/cabinets médicaux avec de nouvelles propositions de contrats respectant les nouvelles exigences légales.
- Dans le domaine médical, les sous-traitants sont p. ex. : les laboratoires, Medidata, les prestataires pour les logiciels de facturation et/ou dossier médicaux, Hin, les prestataires externes pour les salaires du personnel et la comptabilité courante si ceux-ci ont un contact avec les données des patients (fiduciaire, etc.), etc.Des modèles de contrat de sous-traitance et des conventions de confidentialité sont mis à disposition par la FMH.
- Le recours à des opérateurs mobiles situés à l'étranger, le recours à des prestataires informatiques, le recours à des prestataires cloud pour les backups, le recours aux prestataires externes pour le ménage/nettoyage si ceux-ci ont des contacts avec les données des patients, ne nécessitent pas de faire signer des contrats de sous-traitance, mais uniquement des conventions de confidentialité aux prestataires, **mais uniquement des conventions de confidentialité aux prestataires.**

4. Le devoir de prendre des mesures organisationnelles et techniques (voir aussi art. 3 nOLPD)

Ce devoir peut s'articuler autour des **obligations suivantes :**

- **La confidentialité:** Les données traitées ne doivent être accessibles qu'aux personnes autorisées. Pour ce faire, trois contrôles sont essentiels : un accès limité aux données strictement nécessaires à l'accomplissement des tâches; un contrôle de l'accès aux locaux et aux installations ; un contrôle de l'utilisation des systèmes de traitement des données et de leur transmission.
- **La disponibilité et l'intégrité:** Les données traitées doivent être fiables et disponibles en tout temps. Les mesures clés incluent un contrôle des supports de données, un contrôle de la mémoire de stockage, un contrôle du transport lorsque les données sont déplacées empêchant toute prise de connaissance, copie, altération des données (ex. cryptage). Les ordinateurs et logiciels sont maintenus à jour, les failles de sécurité sont réparées et les incidents (techniques ou physiques) signalés. Pour les données physiques, les conserver par exemple dans des armoires verrouillables, des locaux avec systèmes d'accès via clés, badges, codes numériques, etc. - pour lesquels seules les personnes autorisées possèdent lesdits accès.
- **La traçabilité:** Les données personnelles traitées doivent pouvoir être tracées par un contrôle de saisie indiquant toute saisie ou modification de données personnelles dans le système; un contrôle de la communication traçant le destinataire de toute donnée personnelle transmise à un tiers; la détection de toute violation de sécurité afin d'atténuer ou éliminer toute conséquence.
- **La tenue d'un registre de traitement:** Les cabinets médicaux et leurs dossiers de patientes et de patients sont régulièrement soumis à cette obligation, puisqu'ils traitent des données sensibles à grande échelle (voir art. 12 nLPD et 24 nOLPD). 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 nomination d'un conseiller à la protection des données:** C'est facultatif pour les médecins et les cabinets médicaux (art. 10 nLPD et 23 nOLPD). Les tâches du conseiller à la protection des données comprennent le conseil d'ordre général et la formation de l'entreprise aux questions touchant la protection des données. Il participe également à l'adoption et à la mise en œuvre des conditions d'utilisation et des règles de protection des données.

5. Le devoir d'annonce en cas de violation de la sécurité des données

- 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 leur disposition une liste de contrôle et une description de la procédure à suivre en cas de violations de la protection des données. Le non-respect de l'obligation d'information peut être sanctionné amende allant jusqu'à CHF 250 000 (art. 60 al. 1 nLPD).

Fin du document. Mis à jour le 21.08.2023

Société Vaudoise de Médecine
Chemin de Mornex 38
1003 Lausanne

021 651 05 05
info@svmed.ch
www.svmed.ch

Nous restons à votre disposition pour répondre à vos questions.
Votre SVM - 21.08.2023