**Plan de protection des données (document type)**

Version 01/2023

Nom du cabinet médical

Adresse

Code postal/lieu

Tél. : +41 XX XXX XX XX

en vigueur à partir du XX.XX.XXXX

Table des matières

[1 Généralités 3](#_Toc149891543)

[1.1 But et finalité du plan de protection des données 3](#_Toc149891544)

[1.2 Documents complémentaires 3](#_Toc149891545)

[2 Fondamentaux 4](#_Toc149891546)

[2.1 Terminologie 4](#_Toc149891547)

[2.1.1 Informations 4](#_Toc149891548)

[2.1.2 Données personnelles 4](#_Toc149891549)

[2.1.3 Personnes concernées 4](#_Toc149891550)

[2.1.4 Traitement 4](#_Toc149891551)

[2.1.5 Communication 4](#_Toc149891552)

[2.1.6 Protection des données 4](#_Toc149891553)

[2.1.7 Sécurité des données 5](#_Toc149891554)

[3 Responsabilités 5](#_Toc149891555)

[3.1 Obligation légale de garder le secret 5](#_Toc149891556)

[4 Principes du traitement des données 6](#_Toc149891557)

[4.1 Traitements de données personnelles 6](#_Toc149891558)

[4.1.1 Conformité au droit 6](#_Toc149891559)

[4.1.2 Proportionnalité 6](#_Toc149891560)

[4.1.3 Finalité 6](#_Toc149891561)

[4.1.4 Transparence 6](#_Toc149891562)

[4.1.5 Sécurité des données 6](#_Toc149891563)

[4.2 Transmission de données personnelles à des tiers 6](#_Toc149891564)

[4.2.1 Principe 6](#_Toc149891565)

[5 Droits des personnes concernées 7](#_Toc149891566)

[5.1 Droit d’accès 7](#_Toc149891567)

[5.2 Droits supplémentaires 7](#_Toc149891568)

[6 Sécurité de l’information 8](#_Toc149891569)

[6.1 Mesures techniques et organisationnelles 8](#_Toc149891570)

[6.1.1 Mesures organisationnelles 8](#_Toc149891571)

[6.1.2 Mesures techniques 8](#_Toc149891572)

[6.1.3 Administration et accès des utilisateurs 8](#_Toc149891573)

[6.1.4 Journal de bord 8](#_Toc149891574)

[6.1.5 Annonce de violations de la protection des données 8](#_Toc149891575)

[7 Tiers mandaté (sous-traitance) 9](#_Toc149891576)

[8 Sensibilisation du personnel 9](#_Toc149891577)

[9 Délais de conservation, archivage et effacement des données 9](#_Toc149891578)

# Généralités

## But et finalité du plan de protection des données

L’objectif du présent plan de protection est de définir les conditions internes et le cadre pour le traitement des données afin de permettre la mise en œuvre adéquate et uniforme des dispositions légales en matière de protection des données et de réduire les risques liés à la sécurité des données traitées.

Le plan de protection des données vise notamment à :

* assurer la transparence des traitements de données,
* définir les conditions-cadres et la marche à suivre concrète (instructions),
* garantir une utilisation sécurisée des technologies de l’information et de la communication.

Parallèlement, le plan de protection atteste du respect des dispositions en matière de protection des données.

## Documents complémentaires

Les documents suivants font partie intégrante du plan de protection des données :

* [Guide pour le registre des activités de traitement](https://www.fmh.ch/files/pdf28/guide-pour-le-registre-des-activites-de-traitement.pdf)
* [Déclaration de protection des données](https://www.fmh.ch/files/doc3/declaration-de-protection-des-donnees.docx)
* [Déclaration de consentement](https://www.fmh.ch/files/doc3/declaration-de-consentement-formulaire-patientele.docx)
* [Convention de confidentialité](https://www.fmh.ch/files/doc3/convention-de-confidentialite.docx)

# Fondamentaux

## Terminologie

Les définitions et la terminologie sont tirées ou inspirées de la législation actuelle (loi sur la protection des données, LPD). Elles permettent à toutes les parties concernées d’utiliser le même vocabulaire pour une compréhension commune.

### **Informations**

Sont réputées informations tous les relevés ou enregistrements, quels que soient leur forme, leur présentation et leur support.

### **Données personnelles**

Par données personnelles, on entend les informations concernant une personne identifiée ou identifiable. Les *données sensibles* sont un sous-ensemble des données personnelles. Elles se réfèrent aux données sur la santé et aux données génétiques ou biométriques.

### **Personnes concernées**

Les personnes concernées sont des personnes physiques dont les données (données personnelles) font l’objet d’un traitement.

### **Traitement**

Par traitement, on entend toute opération relative à des données personnelles, notamment leur collecte, conservation, utilisation, modification, communication ou destruction.

### **Communication**

Par communication, on entend le fait de rendre des données personnelles accessibles, soit en permettant de les consulter, en les transmettant ou en les publiant.

### Protection des données

La protection des données se réfère au traitement de données personnelles. L’objectif de la protection des données est de protéger les droits de la personnalité et les droits fondamentaux des personnes dont les données font l’objet de traitements.

### Sécurité des données

La sécurité des données ou sécurité de l’information se réfère à toutes les mesures visant à protéger les informations et les données au moyen de mesures organisationnelles et techniques. Elle vise à réduire les risques liés au traitement des données (perte, modification ou prise de connaissance non autorisée, etc.).

# Responsabilités

Toutes les personnes employées au cabinet médical et toutes celles mandatées sont personnellement responsables du traitement des données relevant de leur domaine d’activité. Elles sont tenues de respecter les directives en matière de protection des données et de sécurité de l’information (contrat de travail, contrat de mandat et/ou contrat de prestation).

## Obligation légale de garder le secret

Toutes les personnes employées au cabinet médical et toutes celles mandatées sont tenues de garder le secret. Les médecins et leurs auxiliaires médicaux sont soumis au secret professionnel (art. 321 CP). La violation du secret professionnel est punissable.

L’obligation de garder le secret est inscrite dans les contrats de travail, les contrats de mandat ou les contrats de prestation. Elle continue de s’appliquer après la fin d’un contrat.

# Principes du traitement des données

## Traitements de données personnelles

Les principes ci-dessous doivent être respectés pour le traitement des données personnelles.

### Conformité au droit

Le traitement de données personnelles est conforme à la loi si les conditions-cadres de la loi sur la protection des données (LPD) sont respectées (cf. points 4.1.2 - 4.1.5) ou s’il existe un motif justificatif (p. ex. le consentement des personnes concernées).

### Proportionnalité

Le traitement des données personnelles est possible pour autant qu’il soit approprié et nécessaire à l’exécution des tâches.

### Finalité

Les données personnelles ne peuvent être utilisées que dans le but fixé initialement. Toute autre utilisation exige le consentement de la personne concernée ou une base juridique.

### Transparence

Les processus de traitement des données doivent être transparents et compréhensibles. Cela concerne notamment la collecte des données, qui est généralement effectuée auprès de la personne concernée. Celle-ci a un droit d’accès à ses données (cf. point 5.1).

### Sécurité des données

La mise en place de mesures techniques et organisationnelles appropriées permet de garantir une sécurité des données adaptée au degré de sensibilité des informations et des données personnelles traitées.

## Transmission de données personnelles à des tiers

### Principe

Les données personnelles peuvent être transmises à des tiers si une base légale l’autorise (par ex. LAMal) ou si la personne concernée a donné son consentement.

# Droits des personnes concernées

## Droit d’accès

Toutes les personnes dont les données sont traitées par le cabinet médical ont un droit d’accès à leurs données (art. 25 LPD). Les renseignements demandés par écrit sont fournis par écrit (p. ex. copies), mais ils peuvent aussi être communiqués oralement. Dans les deux cas, il faut vérifier l’identité de la personne concernée.

Les données sur la santé de la personne concernée peuvent lui être communiquées par l’intermédiaire d’un professionnel de la santé qu’elle aura désigné.

En cas d’intérêt privé ou public prépondérant, l’accès aux données peut être limité ou différé.

L’accès ou la décision motivée de limiter le droit d’accès est fourni dans un délai de 30 jours à compter de la réception de la demande d’information.

Pour en savoir plus, veuillez consulter les « Instructions relatives aux demandes de renseignements et de remise de données personnelles »[[1]](#footnote-2)

## Droits supplémentaires

Les personnes concernées disposent de droits supplémentaires, tels que le droit à la rectification de données inexactes ou le droit à la destruction des données traitées de manière non conforme au droit.

# Sécurité de l’information

## Mesures techniques et organisationnelles

Les mesures relevant de la protection des données et de la sécurité de l’information sont planifiées en tenant compte des meilleures pratiques et des standards reconnus.

### Mesures organisationnelles

Les points auxquels le personnel du cabinet doit faire attention lors de l’emploi des outils informatiques sont réglés dans les documents établis par l’équipe informatique.

### Mesures techniques

Les mesures techniques mises en place correspondent à l’état actuel de la technique (cf. les recommandations de la FMH « Exigences minimales pour la sécurité informatique des cabinets médicaux »[[2]](#footnote-3)).

### Administration et accès des utilisateurs

L’administration et l’accès des utilisateurs, assortis des processus et des responsabilités respectifs, sont définis selon un plan des droits d’accès et des rôles.

### Journal de bord

Les mouvements relatifs aux accès et le traitement des données dans les systèmes du cabinet médical sont inscrits dans un journal de bord, ce pour des raisons de sécurité mais aussi pour garantir le respect des dispositions légales en matière de protection des données.

### Annonce de violations de la protection des données

Les violations de la protection des données doivent être immédiatement annoncées au responsable du cabinet médical qui décide des mesures à prendre (par exemple, faire appel à un soutien externe). Il évalue s’il est nécessaire d’informer les personnes concernées et/ou l’autorité de protection des données compétente (PFPDT) (en cas de risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées) (art. 24 LPD).

Cf. le document « Liste de contrôle et déroulement de la procédure en cas de violation de la protection des données »[[3]](#footnote-4).

# Tiers mandaté (sous-traitance)

Pour que le traitement des informations et des données personnelles puisse être confié à un tiers (p. ex. mandataire, prestataire informatique, etc.), les conditions suivantes doivent être remplies :

• les données sont traitées uniquement comme le cabinet serait autorisé à le faire, et

• aucune obligation légale ou contractuelle de confidentialité ne s’oppose à la transmission des données au tiers.

Il faut en particulier prendre les mesures minimales suivantes concernant les prestataires informatiques externes et leur personnel (par ex. administrateurs de banques de données ou de réseaux) :

* + conventions fixant les obligations de confidentialité et les droits d’instruction et de contrôle du cabinet médical vis-à-vis du prestataire externe et de son personnel ;
	+ déclarations de confidentialité valides et signées par le personnel du prestataire externe ;
	+ réglementation univoque de l’étendue des droits d’accès aux systèmes et aux données ;
	+ la traçabilité des activités externes sur les systèmes doit être assurée au moyen de mesures organisationnelles et techniques appropriées (p. ex. principe du double contrôle, journal de bord, etc.).

# Sensibilisation du personnel

Le plan de protection des données, la manière de gérer les données sensibles et le secret professionnel sont présentés de manière appropriée et pertinente aux nouveaux collaborateurs lors de leur entrée en fonction.

En signant leur contrat de travail, les membres du personnel confirment avoir lu et compris ces dispositions et s’y conformer.

Le personnel est régulièrement sensibilisé aux questions de protection et de sécurité des données.

# Délais de conservation, archivage et effacement des données

Les principes concernant la durée de conservation, l’archivage et l’effacement ou la destruction des données personnelles et des informations font partie des dispositions légales importantes.

Pour plus de détails, veuillez consulter le « Guide pour la conservation et l’archivage »[[4]](#footnote-5)

1. https://www.fmh.ch/files/pdf29/instructions-relatives-aux-demandes-de-renseigneme.pdf [↑](#footnote-ref-2)
2. https://www.fmh.ch/fr/prestations/ehealth/securite-informatique.cfm [↑](#footnote-ref-3)
3. https://www.fmh.ch/files/pdf29/liste-de-controle-et-deroulement-de-la-procedure-en-cas-de-violation-de-la-pr.pdf [↑](#footnote-ref-4)
4. https://www.fmh.ch/files/pdf28/guide-pour-la-conservation-et-larchivage.pdf [↑](#footnote-ref-5)