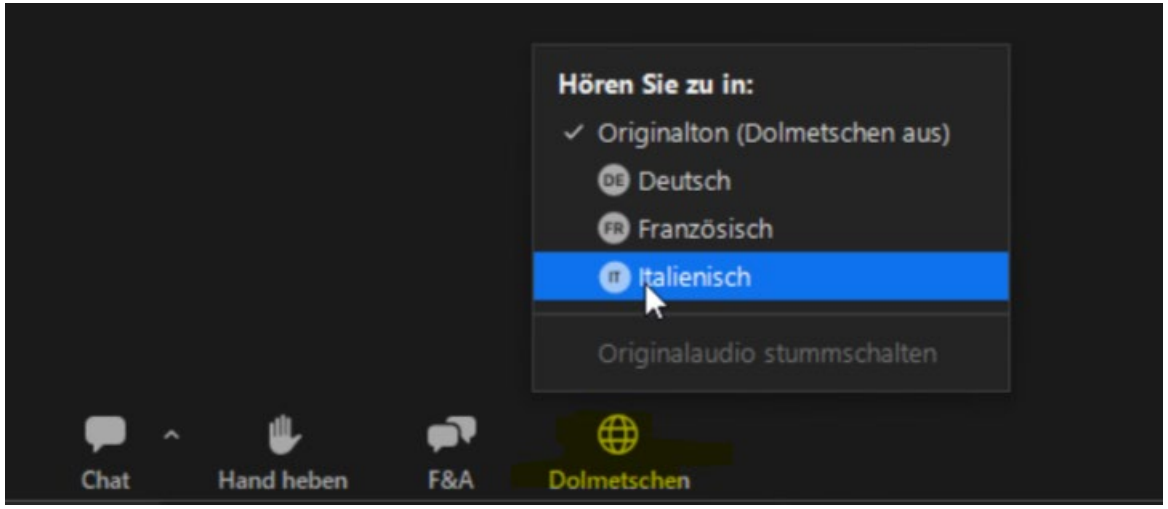
Webinaire de la FMH : nouvelle loi sur la protection des données

Nuova legge sulla protezione dei dati / neues Datenschutzgesetz

Traduction en français et en italien



Les intervenant-e-s :

Bruno Baeriswyl, Dr en droit
Conseiller externe à la protection des données de la FMH

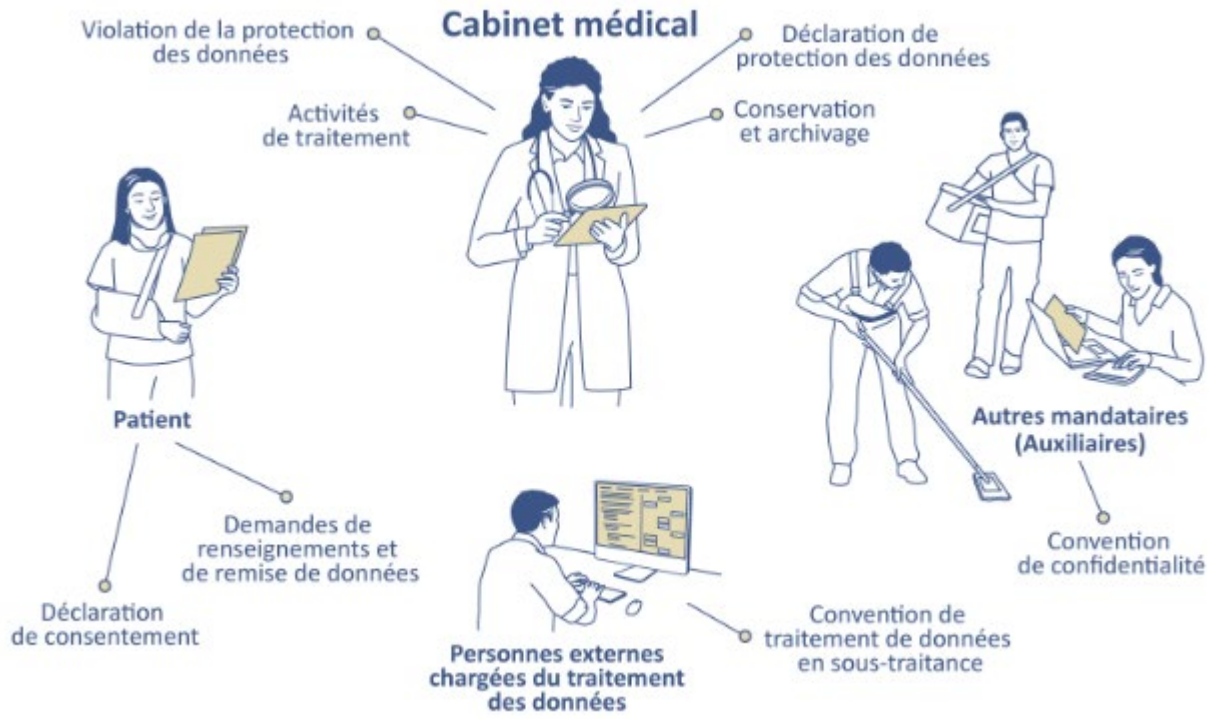
Iris Herzog-Zwitter, Dre en droit
Service juridique de la FMH

Reinhold Sojer, Dr rer. biol. hum.
Chef de la division
Numérisation / eHealth, FMH

Programme

SUJET	INTERVENANT-E	DURÉE (MIN)
Accueil et introduction	R. Sojer	5
Objectifs de la LPD révisée	B. Baeriswyl	5
Principales nouveautés	I. Herzog-Zwitter	5
Terminologie : nouveaux termes importants de la LPD	B. Baeriswyl	5
Déclaration de consentement	I. Herzog-Zwitter	5
Dispositions pénales	B. Baeriswyl	10
Traitement de données en sous-traitance	B. Baeriswyl	5
Aspects juridiques de la responsabilité	I. Herzog-Zwitter	5
Trois nouveautés importantes	B. Baeriswyl	15
Protection et sécurité des données	R. Sojer	25
Table ronde	Toutes et tous	30
Conclusion	R. Sojer	5

Vue d’ensemble des documents mis à disposition



Objectifs de la LPD révisée

Loi sur la protection des données (LPD) du 25 septembre 2020

En vigueur depuis le 1er septembre 2023

Objectifs de la loi (révisée) sur la protection des données (1)

1993 → 2023

Développement technologique

- Traitements des données
  - Pas d'internet
  - Pas de smartphone
  - Pas de cloud
  - Etc.

→ Adaptation aux développements technologiques

Évolution du droit européen

- Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel
  (Convention 108+ du Conseil de l'Europe)
- Protection des données dans le domaine police et justice
  (Directives de l'UE 2016/680)
- Droit général de la protection des données de l'UE
  (Règlement général sur la protection des données, RGPD)

→ Adaptation aux développements juridiques

Objectifs de la loi (révisée) sur la protection des données (2)

Thèmes principaux

Transparence plus élevée concernant les traitements de données

Définition claire des responsabilités (« accountability »)

Mesures de sécurité des données basées sur les risques

Renforcement des droits des personnes concernées

Surveillance renforcée de l'autorité de protection des données (PFPDT) et sanctions pénales

→ Pas de changement du concept de base

Principales nouveautés

en vigueur depuis le 1er septembre 2023

La base pour se protéger en matière de protection des données est d’avoir une vue d’ensemble des données qui sont traitées !

Les principes relatifs au traitement des données sont les mêmes dans l'ancienne et la nouvelle loi sur la protection des données.

Principes relatifs au traitement des données :
conforme au droit, le traitement doit être de bonne foi et proportionné, principe de finalité, les données sont détruites ou anonymisées dès qu'elles ne sont plus nécessaires au regard des finalités du traitement, exactitude, consentement, sécurité des données

Principales nouveautés

1	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. À partir du 1er septembre 2023, seules les données personnelles des personnes physiques sont concernées.
2	Pour chaque collecte de données personnelles, la personne concernée doit être préalablement informée. C'est le responsable du traitement qui l'informe de manière adéquate.
3	Selon la LPD, toute personne peut demander au responsable du traitement si des données personnelles la concernant sont traitées.
4	Le responsable du traitement est tenu de mettre en place des mesures techniques et organisationnelles afin que le traitement respecte les prescriptions de protection des données.
5	De la même manière, les responsables du traitement et les sous-traitants doivent assurer une sécurité adéquate des données personnelles par rapport au risque encouru.

Principales nouveautés

6	Registre des activités de traitement dans certaines conditions. Le Conseil fédéral prévoit des exceptions pour les entreprises qui emploient moins de 250 collaborateurs et dont le traitement des données présente un risque limité d'atteinte à la personnalité des personnes concernées.
7	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. L'analyse d'impact n'est obligatoire qu'en cas de modification des traitements de données antérieurs au 1er septembre 2023.
8	Obligation d'annoncer les cas de violation de la sécurité des données.
9	Dispositions pénales plus sévères : la nouvelle loi sur la protection des données prévoit des amendes pouvant aller jusqu'à 250 000 francs pour les personnes privées. Fournir des renseignements inexacts ou refuser de collaborer sont des actes punissables si c'est intentionnel mais non si c'est par négligence. Délits sur plainte !

Dans la mesure où les dispositions légales en matière de protection des données ont déjà été mises en œuvre dans votre cabinet, celui-ci est, selon toute vraisemblance, protégé en matière de protection des données. Il suffit de procéder à des adaptations en fonction des principales nouveautés.

Terminologie

Nouveaux termes importants de la LPD

Termes

Responsable du traitement
- détermine les finalités et les moyens du traitement de données personnelles

Sous-traitant
- traite des données personnelles pour le compte du responsable du traitement

Données personnelles sensibles (données sensibles)
- not. données sur la santé, désormais aussi données génétiques, données biométriques

Violation de la sécurité des données
- toute violation de la sécurité entraînant de manière accidentelle ou illicite la perte de données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisé à ces données

Consentement

Élément central : autodétermination informationnelle

Consentement

- Lorsque le cadre légal est donné, comme par exemple par l'assurance-invalidité ou l'assurance-accidents, il n'est pas explicitement nécessaire d'obtenir un consentement, car la signature du formulaire de demande de l'AI, par exemple, équivaut à une légitimation.

- C'est différent en droit privé (p. ex. contrat thérapeutique) et en droit des assurances privées. Dans ce cas, une déclaration de consentement est nécessaire.

Consentement

- En cas de traitement de données sensibles, le patient doit donner explicitement son consentement, soit oralement, soit par écrit. Mais c'était déjà le cas avec l'ancienne loi sur la protection des données.

Consentement

- Le consentement doit être sans équivoque et la volonté de la personne concernée doit être exprimée de manière claire dans sa déclaration.
- Conformément au principe de proportionnalité, le consentement doit être d'autant plus clair que les données personnelles en question sont sensibles.
- En principe, le consentement peut être donné sans forme particulière et n'est pas soumis à l'obligation d'être écrit.

Dispositions pénales

Dispositions pénales (1)

Remarques préliminaires

La principale disposition pénale :

→ secret professionnel ; secret médical (art. 321 CP)

La mauvaise comparaison :

→ Dans l'UE (RGPD), l'autorité de protection des données dispose de possibilités de sanctions étendues (« amendes »). La Suisse dispose de beaucoup moins de dispositions pénales.
(L'ancienne loi sur la protection des données fixait déjà des dispositions pénales. Les condamnations fondées sur ces dispositions sont pratiquement inexistantes).

Dispositions pénales (2)

Conditions de la punissabilité

Infractions objectives

- Violation des obligations d'informer, de renseigner et de collaborer (art. 60 LPD)
- Violation des devoirs de diligence (art. 61 LPD)
- Violation du devoir de discrétion (art. 62 LPD)
- Insoumission à une décision (art. 63 LPD)

Infractions subjectives

- Faute intentionnelle (« avec conscience et volonté »)

Plainte pénale (sauf art. 63 LPD)

- Dans les trois mois suivant la prise de connaissance

Peine encourue

- Amende (max. 250 000 francs) → contravention

Poursuites pénales

- Cantons

Traitement de données en sous-traitance

Traitement de données en sous-traitance - convention de confidentialité

Traitements de données en sous-traitance

Responsabilités

Sous-traitance
→ p. ex. externalisation de l'informatique

La responsabilité en matière de protection des données reste celle du *responsable* !

- Choix, instruction et surveillance du sous-traitant
- Directives relatives au traitement des données pour le sous-traitant
- Le sous-traitant doit être en mesure d'assurer la sécurité des données

→**Convention de traitement de données en sous-traitance**

Communication de données
→ p. ex. à l'orthoprothésiste

La responsabilité en matière de protection des données est transférée à l'orthoprothésiste.

- Le responsable (initial) est chargé de sécuriser la transmission
- Si le destinataire n'est pas soumis au secret professionnel, il doit veiller au respect de la confidentialité

→**Convention de confidentialité**

Aspects juridiques de la responsabilité

Aspects juridiques de la responsabilité

- Dans le cadre du contrat thérapeutique, le médecin doit répondre de tout manquement à son devoir de diligence.
- Il faut donc se baser sur une application de la diligence adaptée à chaque acte spécifique à la profession.
- La diligence requise dans l'exécution du contrat porte sur le choix (cura in eligendo), l'instruction (cura in instruendo) et la surveillance (cura in custodiendo).

Aspects juridiques de la responsabilité

- Le devoir de diligence du médecin comprend la fourniture d'un équipement adapté et du matériel et des instruments adéquats pour les auxiliaires, mais aussi l'organisation pertinente et appropriée des processus de travail et de l'entreprise.

- Pour éviter le fameux dommage causé à un tiers, le médecin doit, si nécessaire, procéder à un contrôle final des processus de travail.

- En matière de responsabilité civile, la preuve libératoire est apportée lorsque l'on prouve que l'on a agi avec toute la diligence requise par les circonstances pour éviter un dommage de cette nature ou que le dommage serait de toute façon survenu même si l'on avait fait preuve de cette diligence.

Aspects juridiques de la responsabilité

Exemples

- Faute d'information, le consentement est insuffisant.
- Les registres de données exigés par la loi doivent être à jour et complets.
- Les responsabilités et les procédures au sein d'un cabinet doivent être organisées.
- La formation et l'instruction des collaborateurs doivent être assurées.
- Le sujet de la responsabilité est la personne responsable de la violation de la loi sur la protection des données. Selon le message relatif à la révision de la loi, ce ne sont pas les responsables de l'action incriminée qui sont visés, mais les responsables de l'organisation.

Trois nouveautés importantes

Registre des activités de traitement
Annonce des violations de la sécurité des données
Analyse d’impact relative à la protection des données personnelles

Registre des activités de traitement

Documentation des processus de traitement de données
→ Grande quantité de données personnelles sensibles (p. ex. données sur la santé) : pas d'exception

Contenu (« indications minimum ») :

- l'identité du responsable du traitement ;
- la finalité du traitement ;
- une description des catégories de personnes concernées et des catégories de données personnelles traitées ;
- les catégories de destinataires ;
- dans la mesure du possible, le délai de conservation des données personnelles ou les critères pour déterminer la durée de conservation ;
- dans la mesure du possible, une description générale des mesures visant à garantir la sécurité des données ;
- en cas de communication de données personnelles à l'étranger, le nom de l'État concerné et les garanties.

→ Modèle de registre des activités de traitement

Annonce des violations de la sécurité des données

Obligation d'annoncer en cas de « risque élevé »

- p. ex. perte de données de santé ou accès non autorisé

Annonce au Préposé fédéral à la protection des données et à la transparence (PFPDT)
- Annonce en ligne : https://databreach.edoeb.admin.ch/report

Éventuelle information des personnes concernées (→ si nécessaire pour leur protection)

→ Liste de contrôle et déroulement de la procédure en cas de violation de la protection des données

Analyse d’impact relative à la protection des données personnelles

Lors de nouveaux traitements de données
(Traitements de données existants : catégories de données supplémentaires / autres finalités)

Risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées
- Utilisation de nouvelles technologies
- Traitement de données sensibles à grande échelle

→ Évaluation des risques (et planification des mesures techniques et organisationnelles appropriées)

Consultation préalable du PFPDT (art. 23 LPD)
- Risque élevé malgré les mesures prévues
- Pas de consultation préalable si conseiller à la protection des données

Délais de conservation / effacement

Les données personnelles doivent être détruites ou anonymisées

- dès qu'elles ne sont plus nécessaires au regard des finalités du traitement

Définir le délai de conservation des données ou les critères pour déterminer la durée de conservation

- Dispositions légales

→ Guide pour la conservation et l'archivage

Protection et sécurité des données

Mesures techniques et organisationnelles

Sécurité des données

Art. 8 Sécurité des données

[1] Les responsables du traitement et les sous-traitants doivent assurer, par des mesures organisationnelles et techniques appropriées, une sécurité adéquate des données personnelles par rapport au risque encouru.

[2] Les mesures doivent permettre d'éviter toute violation de la sécurité des données.

[3] Le Conseil fédéral édicte des dispositions sur les exigences minimales en matière de sécurité des données.

Sécurité des données

Protection des données dès la conception

Art. 7 Protection des données dès la conception et par défaut

[1] Le responsable du traitement est tenu de mettre en place des mesures techniques et organisationnelles afin que le traitement respecte les prescriptions de protection des données, en particulier les principes fixés à l'art. 6. Il le fait dès la conception du traitement.

Sécurité des données

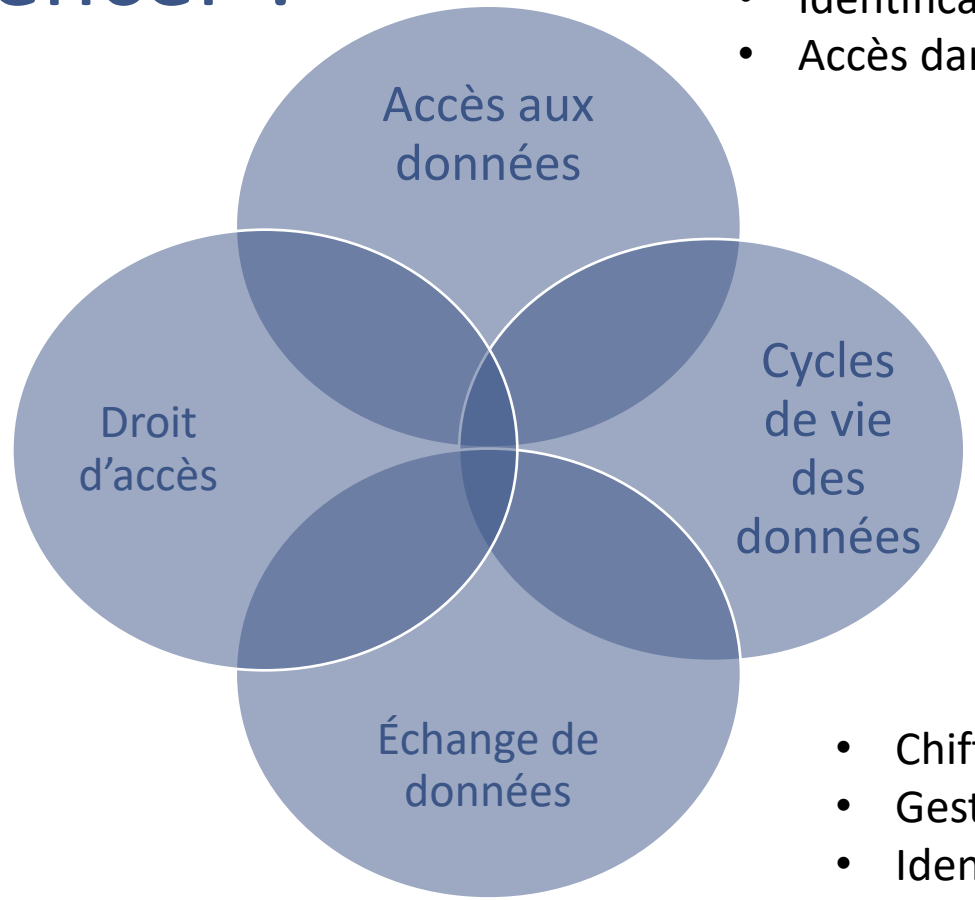
L’art. 7, al. 1, fonde l’obligation de diligence du responsable du traitement.
L’art. 8, al. 1, impose des obligations aux deux parties, responsable du traitement et sous-traitant !

« Le responsable du traitement doit s’assurer activement que le sous-traitant respecte la loi dans la même mesure que lui-même. »

« Il est donc tenu de le choisir avec diligence, de lui donner des instructions appropriées et de le surveiller autant que nécessaire. »

Par où commencer ?

- Sécurité des locaux, salles de serveurs, postes de travail
- Identification et authentification
- Accès dans et hors cabinet médical



- Processus pour les demandes d'accès
- Effacement de données
- Journal de bord

- Collecte et journal de bord
- Anonymisation
- Chiffrement
- Sécurité des données
- Sous-traitance (p. ex. cloud)
- Classification des données

- Chiffrement du transport et du contenu
- Gestion des clés
- Identité électronique
- Journal de bord

Recommandations

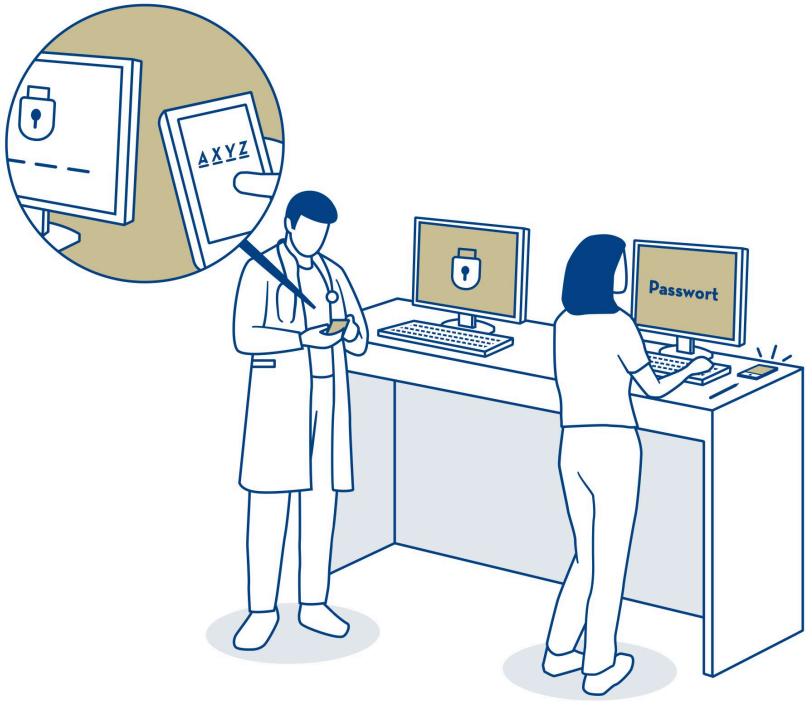
Recommandations du PFPDT

Exigences techniques et organisationnelles pour les services sur le cloud

Exigences minimales pour la sécurité informatique

Exemple « Réguler et protéger l'accès »

L'administration centralisée et l'attribution structurée des droits d'accès et d'utilisation, par exemple via Active Directory ou d'autres services, minimisent les risques d'accès non autorisé aux données sensibles par des parties internes ou externes. La gestion régulière des droits d'accès et d'utilisation permet d'enregistrer et d'ajouter les changements au fur et à mesure que les employés entrent en fonction ou quittent leurs fonctions.

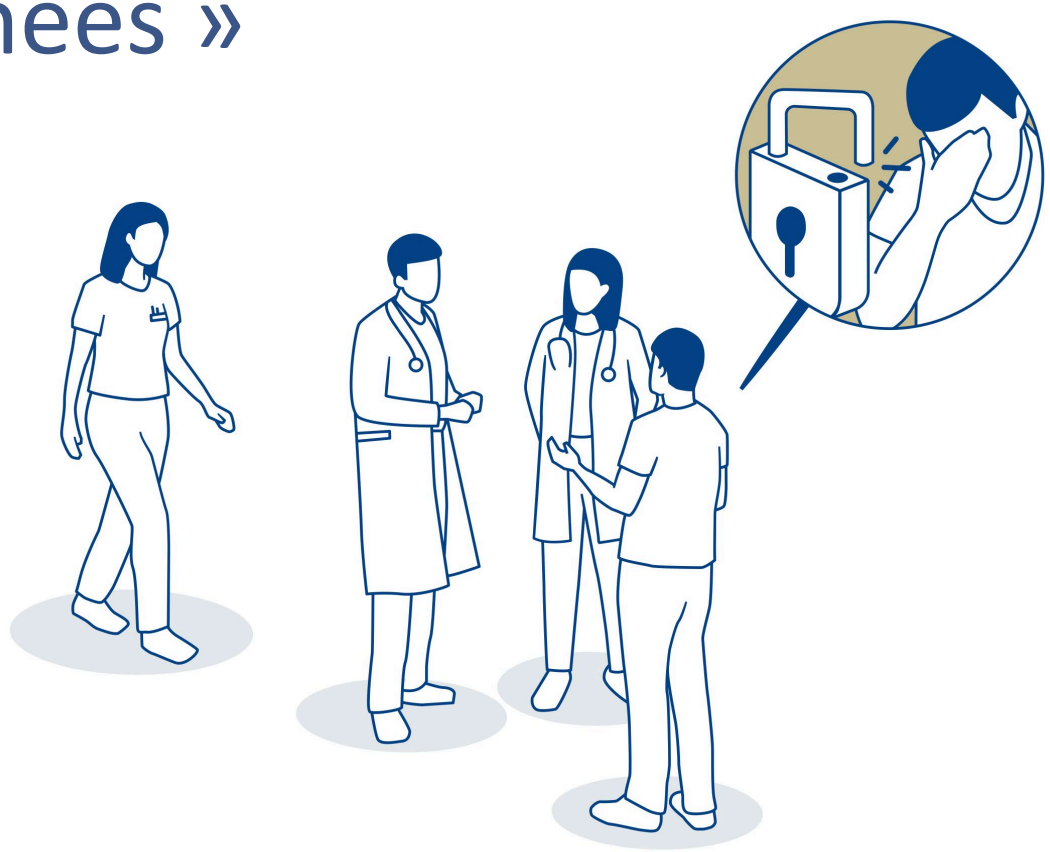


Mesures

- Comptes d'utilisateur personnels pour les collaborateurs
- Limitation des droits des utilisateurs (« Need to know »)
- Accès au réseau interne du cabinet avec authentification préalable forte
- Changement de mot de passe

Exemple « Sensibiliser les collaborateurs du cabinet médical à la sécurité des données »

Le personnel d'un cabinet médical est une cible privilégiée, c'est pourquoi les attaques utilisent souvent l'ingénierie sociale pour accéder à l'environnement informatique et aux données. Pour s'en prémunir, il est primordial de sensibiliser le responsable et le personnel du cabinet.

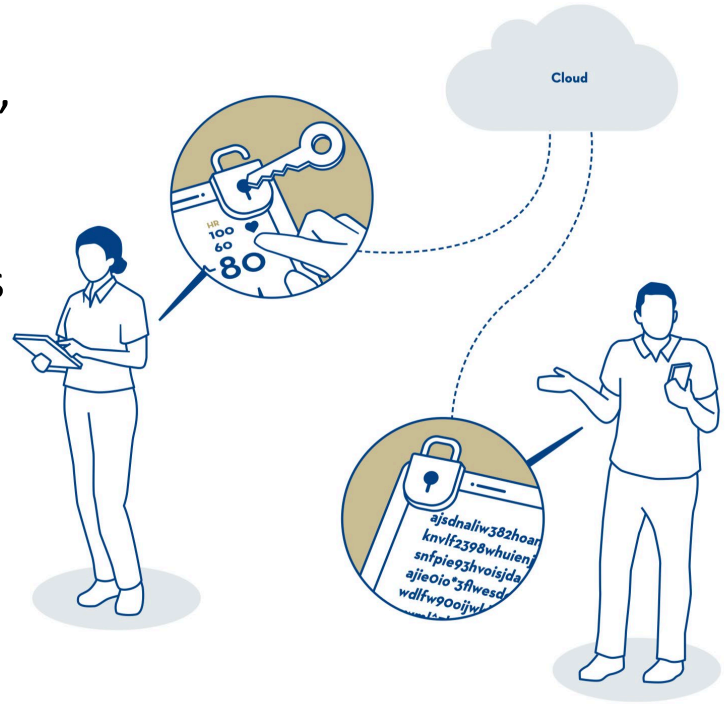


Mesures

- Aborder ces questions lors des réunions d'équipe (mots de passe, classification des données, utilisation de l'informatique, gestion et échange de données, procédure en cas d'incidents de sécurité)
- Former les nouvelles personnes, fiches d'information
- Utilisation de l'informatique à titre privé
- …

Exemple « Chiffrement et gestion des clés (cloud) »

Les données sauvegardées (Data at Rest) et les données en transit (Data in Transit) doivent être protégées par chiffrement. De même, la communication sur tous les raccordements entrants et sortants vers et depuis l'infrastructure sur le cloud, y compris les interfaces au sein de cette infrastructure, doit être chiffrée et avoir lieu après authentification.



Mesures

- Stockage chiffré des données de contenu dans tous les cycles de vie
- Gestion des clés (gestion de récupération efficace)
- Transport chiffré

Définir les responsabilités et fixer les directives informatiques

Le responsable fixe les directives, les processus et le contrôle de validation interne, entre autres :

- contrôles d'accès
- collecte, enregistrement et effacement des données
- respect des exigences réglementaires
- gestion des risques
- autres

Si le traitement des données est externalisé sur le cloud, la gouvernance reste toujours en main du cabinet médical. La gouvernance ne peut pas être externalisée à un prestataire externe.

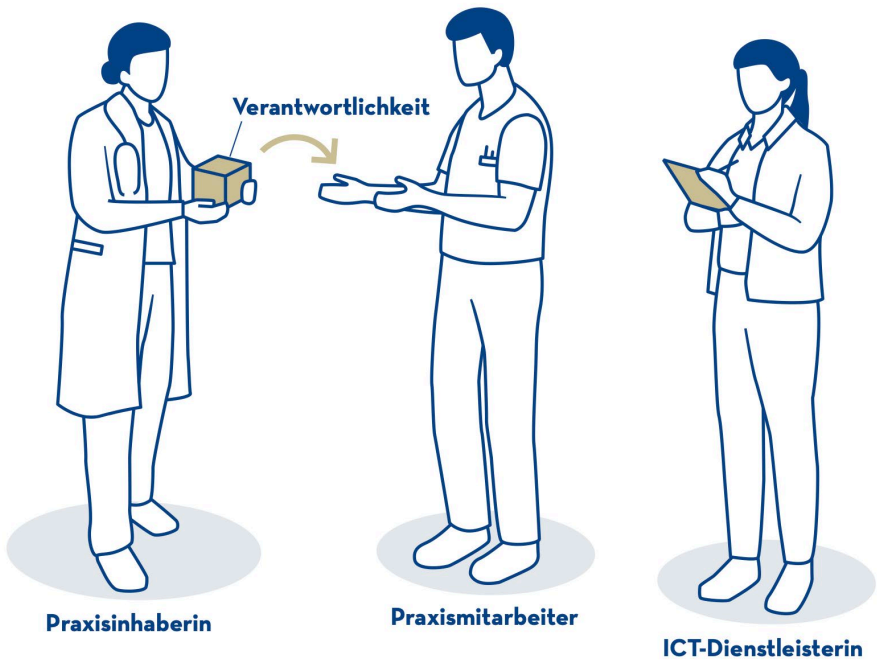


Table ronde

Table ronde

Questions choisies

Conclusion

Conclusion

- Le webinaire est enregistré : envoi d’un courriel avec le lien vers l’enregistrement
- Présentation disponible en français, allemand et italien

Merci de votre attention !

FMH · Verbindung der Schweizer Ärztinnen und Ärzte · Fédération des médecins suisses
Postfach · CH-3000 Bern 16 · Telefon +41 31 359 11 11
info@fmh.ch · www.fmh.ch