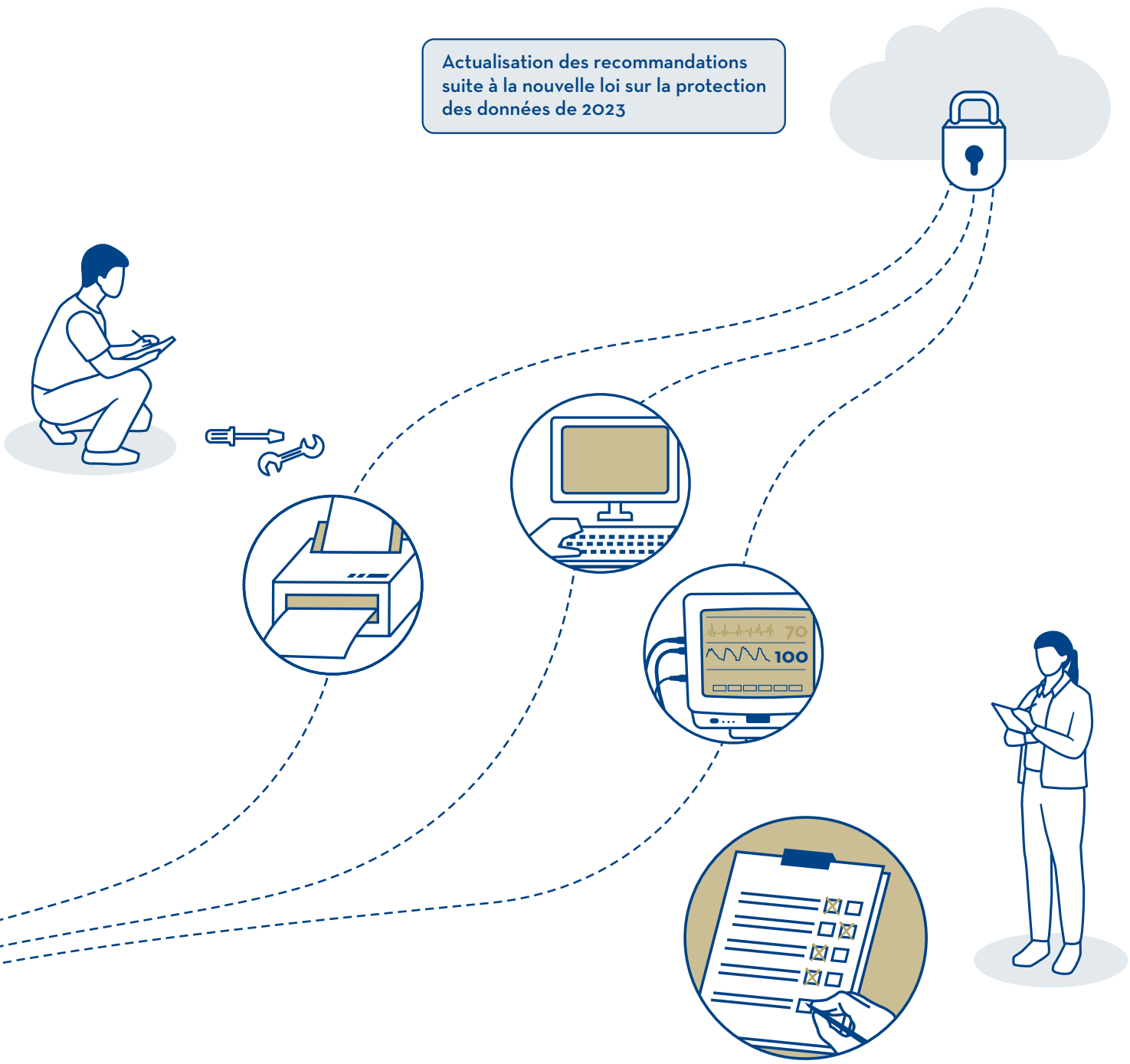
FMH

D3

Sécurité informatique des cabinets médicaux

Onze recommandations

Actualisation des recommandations suite à la nouvelle loi sur la protection des données de 2023



Sommaire

Les présentes recommandations ont été adaptées pour qu'elles restent sur le fond compatibles avec la loi révisée sur la protection des données entrée en vigueur le 1er septembre 2023.

Introduction

La transformation numérique et les interconnexions accrues dans l'environnement des soins de santé ouvrent de nouvelles perspectives, par exemple pour améliorer la qualité des traitements et l'efficacité des processus, mais comportent également de nouveaux risques dans le domaine de la sécurité et de la protection des données. Les cyberattaques contre les données de santé et les infrastructures informatiques peuvent porter atteinte à la vie privée des patientes et des patients, restreindre considérablement les activités quotidiennes d'un cabinet médical, lui causer un préjudice financier et nuire à sa réputation ou influencer le traitement des patients.

En revanche, disposer de données électroniques constitue un facteur de succès important lorsqu'il s'agit d'accroître l'efficacité d'un cabinet. Les collaboratrices et les collaborateurs sont, dans le cadre de leur travail, quotidiennement en contact avec les données personnelles très sensibles des patients qu'ils recueillent et stockent sous forme numérique ou analogique. Il appartient donc aux cabinets médicaux de veiller à la protection et à la sécurité de ces données.

La loi fédérale sur la protection des données (LPD) qualifie les données médicales de données personnelles sensibles, si bien que des mesures importantes sont nécessaires pour garantir une protection adéquate. La mise en place, l'entretien et la maintenance d'un environnement informatique sécurisé mais aussi l'élaboration de normes de sécurité et la sensibilisation du personnel à une culture de la sécurité sont des tâches importantes qui exigent des ressources humaines et financières.

Les recommandations exposées ci-après visent à vous aider à garantir la mise en place et le maintien de la protection et de la sécurité des données dans votre cabinet.

Dre Yvonne Gilli

Présidente de la FMH

Groupe cible/destinataires

Les recommandations de la FMH concernent l'organisation et l'infrastructure informatiques de cabinets médicaux de taille petite ou moyenne. Les exigences et les mesures exposées ci-après ont été validées après une série d'entretiens avec des médecins et des propriétaires de cabinet et s'appliquent aux cabinets jusqu'à une douzaine de médecins environ. Elles s'adressent en premier lieu aux médecins, au personnel du cabinet et aux prestataires tiers mandatés (p. ex. prestataires TIC).

But

Les onze recommandations sur la sécurité informatique des cabinets médicaux visent à garantir la sécurité et la protection des données. Elles prennent en compte la taille et la complexité de l'environnement informatique, le nombre de collaborateurs et le profil de risque des cabinets médicaux. Elles ont été établies suite à des entretiens menés avec différents médecins sur la base de questions passant en revue les principes de la loi sur la protection des données et d'autres documents réglementaires. Le degré de détail des recommandations est adapté aux effectifs et ressources disponibles.

Les recommandations de la FMH contribuent à une protection appropriée des données sensibles d'un cabinet médical et répondent aux obligations légales concernant la protection des données personnelles sensibles.

Dangers

Plusieurs facteurs technologiques, organisationnels et humains exposent à différents dangers les données traitées dans un cabinet médical (cf. points 1 à 4). Les menaces potentielles se situent aux points faibles du matériel informatique, des logiciels, des processus ou du comportement des collaborateurs du cabinet. Si ces points faibles servent de porte d'entrée à une attaque informatique, la confidentialité, la disponibilité ou l'intégrité des données médicales et des données des patients risquent d'être compromises. Les dangers peuvent aussi bien être d'ordre technique que le résultat d'un manque de sensibilisation des collaborateurs et des médecins qui deviennent ainsi une cible privilégiée d'attaques d'ingénierie sociale. Le tableau ci-dessous représente l'environnement informatique d'un cabinet médical et indique les interactions avec les prestataires TIC externes, les patients et d'autres institutions de santé. Les cercles jaunes avec les points d'exclamation matérialisent les points de danger possibles.

1. Les logiciels malveillants sont des programmes développés pour exécuter des fonctions non désirées et éventuellement nuisibles sur différents types de terminaux. Il s'agit par exemple de ransomware, également connus sous le nom de rançongiciels ou logiciels d'extorsion, installés sur l'appareil. Ce type de logiciel bloque l'accès aux données et empêche l'utilisation de l'appareil jusqu'à ce qu'un outil de débridage soit envoyé à la victime en échange d'une somme d'argent. Les logiciels malveillants atteignent les appareils via un support de données (clé USB), une pièce jointe (e-mail) ou des services sur le cloud.

2. Les attaques d'ingénierie sociale ciblent les personnes dans le but d'obtenir des informations de carte de crédit ou des mots de passe au moyen de courriels, d'appels ou de messages instantanés censés les induire en erreur pour accéder à leur appareil. Le manque d'attention sur internet ou à la lecture

de son courrier électronique, par exemple avec l'ouverture de pièces jointes, peut enclencher l'installation de programmes malveillants. Par ailleurs, les erreurs humaines peuvent également constituer une menace, par exemple avec l'envoi d'informations sur un patient au mauvais destinataire.

3. L'échange non chiffré de données par courrier électronique entre les médecins, les patient et les acteurs du secteur de la santé offre la possibilité à une personne malintentionnée de lire la communication et d'intercepter des informations sensibles, tout comme les erreurs de destinataire peuvent entraîner leur divulgation.

4. L'utilisation de services sur le cloud pour l'archivage des données primaires ou les back-up constitue une menace potentielle pour la confidentialité et l'intégrité des données car, selon le modèle choisi, il est impossible d'empêcher le fournisseur d'accéder aux données. Le stockage non chiffré sur le cloud ou les téléchargements non chiffrés vers et depuis le cloud offrent la possibilité de cyberattaques en vue d'intercepter ou de visualiser les données. La dépendance du cabinet médical vis-à-vis de son fournisseur et de la solution de cloud computing affaiblit sa position. Les possibilités de vérifier l'accord contractuel concernant la protection, la sécurité, le traitement des données par le fournisseur sont souvent limitées, et la relation se base sur la confiance. Les plateformes à distance (cloud) sont donc des cibles intéressantes et « plus rentables » à attaquer parce que les dommages infligés sont plus importants ou le nombre de données capitalisées, plus élevé.

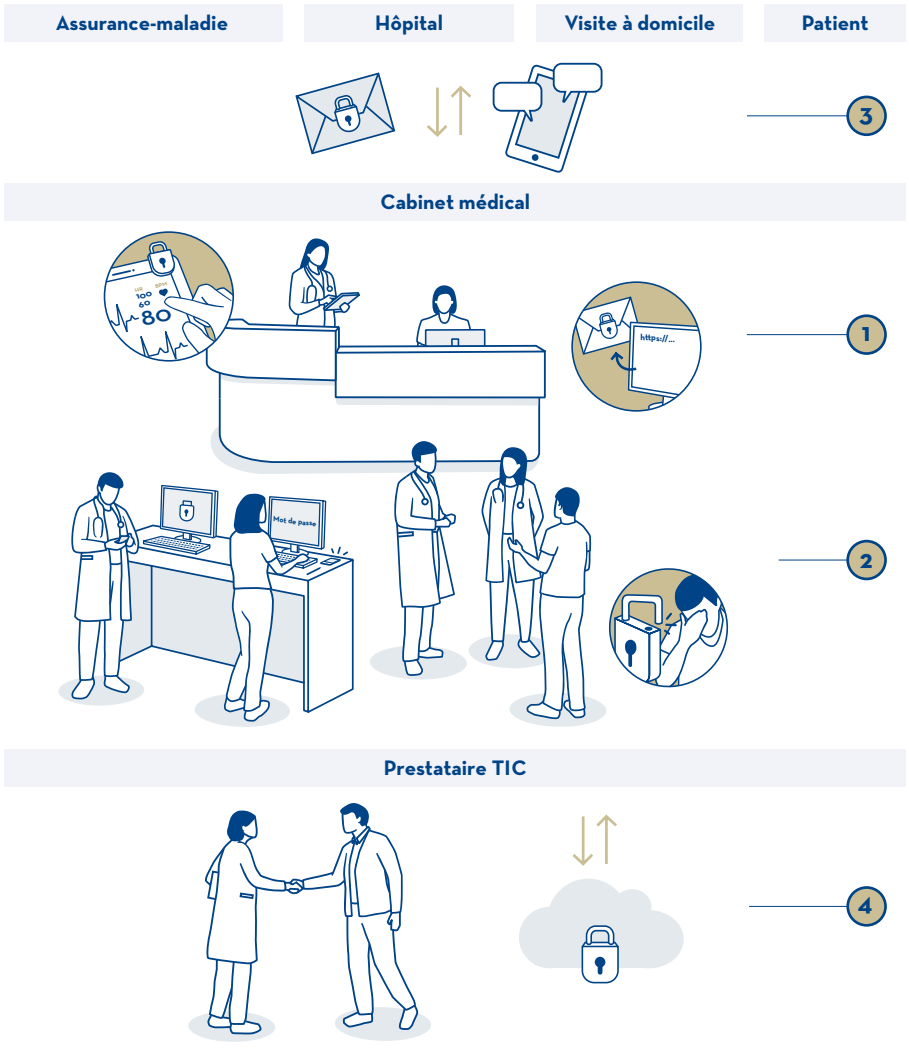


Figure 1
Exemple de l'environnement informatique d'un cabinet médical

Le scénario suivant vise à illustrer, à titre d'exemple, comment les dangers évoqués peuvent se manifester sur le terrain. Les attaques visent principalement à obtenir des données sur lesquelles il est possible de capitaliser ou simplement à extorquer des fonds. Ces objectifs peuvent être atteints de plusieurs façons, par exemple, avec l'envoi d'un courriel contenant un logiciel malveillant intégré dans un document publicitaire/de postulation ou d'un courriel proposant un lien vers un jeu d'argent. En cliquant sur le document en annexe ou sur le lien, le logiciel malveillant est installé sur l'appareil et bloque l'accès à l'ordinateur et à ses ressources. Suite à une telle attaque, la victime est invitée à s'acquitter d'une certaine somme d'argent pour retrouver l'accès à son ordinateur.

Une attaque peut également être déguisée en un service « soi-disant » d'aide d'un concepteur de logiciel qui s'adresse au personnel du cabinet pour demander la vérification des mots de passe et des noms d'utilisateur. Si les employés communiquent ces informations, ils offrent la possibilité à un inconnu d'accéder aux terminaux, pour autant que la structure informatique le permette. Ce type d'attaque, appelé hameçonnage par courriel (phishing) ou hameçonnage par téléphone (vishing), relève de l'ingénierie sociale. Pour atteindre les appareils finaux, l'inconnu rentre dans le cabinet médical sans se faire remarquer ou en prétextant d'attendre quelqu'un. Une fois à l'intérieur, lorsqu'il est sans surveillance, il peut accéder à un ordinateur de la salle d'examen. Un ordinateur déverrouillé, des mots de passe faibles ou des autorisations d'accès étendues lui facilitent l'accès aux données sensibles.

La liste des dangers mentionnés n'est pas exhaustive. Elle va évoluer et s'amplifier avec le temps car le développement de technologies innovantes suscite également des vocations pour développer de nouvelles méthodes d'attaque. Les menaces qui pèsent sur la sécurité et la protection des informations et des données sensibles augmenteront en raison des changements technologiques de plus en plus nombreux aussi bien pour les particuliers que pour le secteur commercial.

Il est indispensable de sensibiliser les médecins et leurs collaborateurs, et tous ceux en contact avec des données et des informations sensibles, à la notion de sécurité au moyen de mesures ciblées. Les modèles habituels de mise à disposition, par exemple, d'une licence permanente (achat unique) pour utiliser un appareil, ne seront très probablement plus proposés à l'avenir et seront remplacés par des solutions sur le cloud.

Caractère obligatoire

Le présent document expose des recommandations permettant d'atteindre une sécurité informatique de base et donc aussi de préserver et garantir une sécurité des données appropriée. Il aide à respecter le niveau légal exigé en matière de protection des données.

Structure du document

La sécurité informatique des cabinets médicaux est exposée en onze recommandations destinées aux médecins installés en cabinet médical, à leurs collaborateurs et aux prestataires TIC externes, et incluent trois documents avec un degré de précision adapté aux groupes cibles.

	D1 Représentation graphique	D2 Programme en 11 points	D3 Mesures détaillées
Médecin/propriétaire du cabinet	○	○	●
Personnel du cabinet	○	○	●
Prestataire TIC	×	×	●

Figure 2
Hiérarchie des documents sur les exigences minimales pour la sécurité informatique et les groupes cibles

Le premier document (D1) est une représentation graphique des onze recommandations. Le deuxième (D2) les récapitule avec quelques indications supplémentaires sur les mesures (programme en onze points). Le troisième document, que vous tenez entre vos mains, détaille les mesures et propose des explications approfondies sur les onze recommandations et les mesures concrètes. La représentation graphique et le programme en onze points s'adressent en premier lieu aux médecins/propriétaires de cabinets médicaux et à leur personnel. Les mesures détaillées (dans le présent document) sont rédigées en priorité pour les prestataires TIC externes mais peuvent également intéresser les médecins/propriétaires de cabinets et leur personnel. Le tableau ci-dessous représente la hiérarchie des documents sur les exigences minimales pour la sécurité informatique et les groupes cibles de chaque document (cf. fig. 2).

La sécurité informatique des cabinets médicaux est déclinée en onze recommandations :
- Recommandation 1 : définir les responsabilités et fixer les directives informatiques (TIC)
- Recommandation 2 : dresser l'inventaire des ressources informatiques
- Recommandation 3 : restreindre les droits d'accès et gérer les utilisateurs
- Recommandation 4 : sensibiliser les collaborateurs à la protection des données
- Recommandation 5 : protéger les appareils contre les logiciels malveillants
- Recommandation 6 : protéger le réseau
- Recommandation 7 : configurer et entretenir l'infrastructure informatique
- Recommandation 8 : assurer des sauvegardes fiables
- Recommandation 9 : assurer la sécurité des données échangées
- Recommandation 10 : définir une procédure de gestion des incidents de sécurité
- Recommandation 11 : mandater des prestataires externes et superviser leur travail

Les recommandations, numérotées de **R1** à **R11** contiennent à la fois des mesures nécessaires et des mesures facultatives.

Les mesures nécessaires sont reconnaissables aux deux types de formulation suivants :
- « Les mots de passe utilisés sont sécurisés. »
- « Seuls des mots de passe sécurisés peuvent être utilisés. »

Les mesures facultatives, qui offrent encore davantage de sécurité, se présentent sous la forme suivante :
- « Il est recommandé d'organiser régulièrement des formations sur la sécurité informatique pour le personnel. »

Pour distinguer les mesures (**M**) des informations (**I**), nous utilisons un numéro d'identification. A titre d'exemple, le numéro **M-1.01** correspond aux éléments suivants :

- **M** : pour mesure
- **1.** : le chiffre avant le point se réfère à la recommandation.
- **.01** : les deux chiffres après le point indiquent le numéro de la mesure.

L'exemple **M-1.01** se réfère donc à la mesure 1 de la recommandation n° 1. et l'exemple **I-1.01** à une information de la mesure **M-1.01**.

Limitations

Le présent document est soumis aux limitations suivantes :

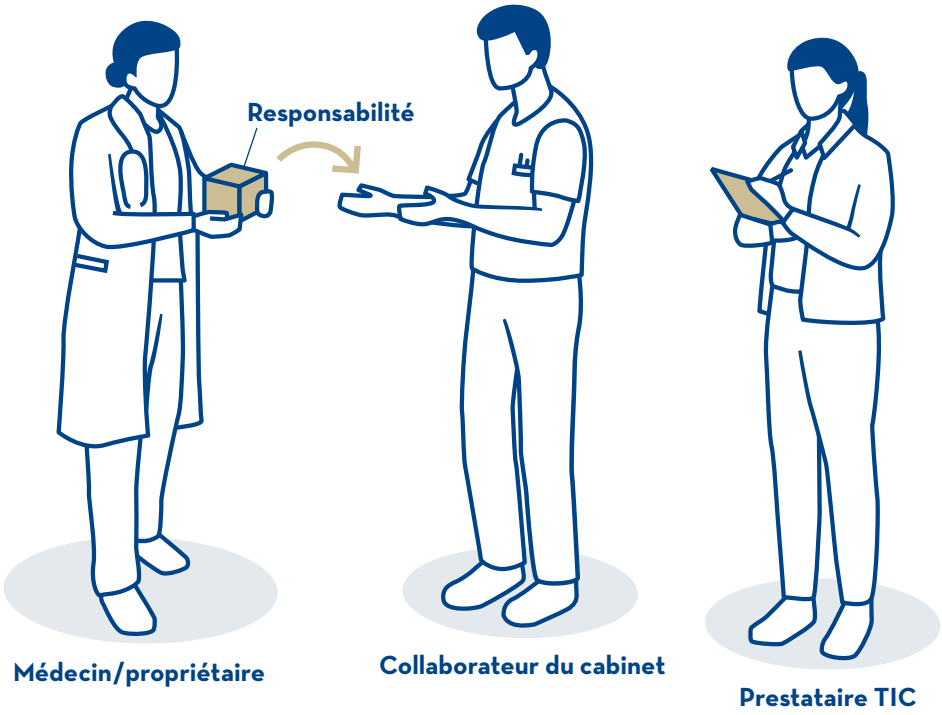
- Les présentes recommandations pour la sécurité informatique se limitent aux aspects techniques et procéduraux de la sécurité des données.
- Elles visent le traitement électronique de données.
- Elles sont indépendantes des exigences de sécurité pour le dossier électronique du patient (DEP).
- Leur mise en œuvre offre une sécurité des données adéquate.

Conditions minimales requises

Il est indispensable que le cabinet médical dispose de locaux offrant une sécurité adéquate, à savoir qu'il réponde aux exigences suivantes :

- Les locaux du cabinet sont équipés d'un accès protégé. En dehors des heures d'ouverture, ils sont fermés à clé et ne sont accessibles qu'aux personnes autorisées. Pendant les heures d'ouverture, le personnel voit systématiquement si une personne pénètre dans le cabinet.
- Les fenêtres et les portes sont fermées en dehors des heures d'ouverture et sont protégées par des mesures supplémentaires en cas de risque d'effraction accru (p. ex. rez-de-chaussée, nombre élevé de cambriolages dans le voisinage).
- Les documents papier contenant des informations sensibles sont conservés dans un meuble fermant à clé. Les personnes non autorisées ne doivent à aucun moment accéder à ces documents.
- Toute personne non autorisée ne doit pas avoir la possibilité de consulter les écrans à l'intérieur du cabinet. Les positionner en conséquence.
- Les serveurs, les composants réseau, la mémoire et les lecteurs amovibles doivent être utilisés et stockés dans une pièce inaccessible aux patients et, si possible, fermée à clé. S'il n'y a pas de pièce séparée, les composants doivent être utilisés dans une armoire spécialement conçue à cet effet pouvant être verrouillée.

R1
Définir les responsabilités et fixer les directives informatiques (TIC)



Introduction

Le responsable du cabinet (le médecin ou le propriétaire) porte l'entière responsabilité de la sécurité et de la protection des données, de l'utilisation de l'environnement informatique et de son personnel. Les deux rôles suivants deviennent incontournables dans l'organisation d'un cabinet médical :

- Responsable de la protection et de la sécurité des données (R-PSD)
- Responsable informatique

Le responsable de la protection et de la sécurité des données (R-PSD) est chargé des consignes de sécurité. Il les fixe et, suivant les cas, les met en œuvre et contrôle si elles sont respectées. Ce rôle peut revenir au propriétaire du cabinet, un prestataire informatique externe ou un membre du personnel ou du corps médical. Le R-PSD détermine qui a accès à quelles données/ressources et gère les droits d'accès.

Le rôle du R-PSD se distingue de celui du responsable informatique qui est chargé de la mise sur pied, du fonctionnement et de la maintenance de l'environnement informatique.

Alors que le premier fixe les exigences en matière de protection et de sécurité des données, le second veille à leur implémentation technique.

Ces deux postes peuvent être attribués à une ou plusieurs personnes.

Le personnel est tenu de respecter les directives de sécurité mises en place par le responsable PSD.

But

Définir les responsabilités a pour but de souligner que la sécurité et la protection des données sont un thème important du cabinet médical et permet de désigner une personne à même de répondre aux questions et de relever les défis.

Mesures

M-1.01 Les rôles de responsable PSD et de responsable informatique et leurs remplaçants respectifs sont attribués.

Les coordonnées des personnes qui occupent ces postes sont communiquées et consignées sur une liste accessible à tous les membres du personnel et du corps médical du cabinet.

M-1.02 Les directives de sécurité internes et les consignes sont développées sur la base des onze recommandations. Elles doivent au moins aborder les thèmes suivants :

- Mots de passe et PIN (cf. **R3 : restreindre les droits d'accès et gérer les utilisateurs**)
- Classification des données : il faut pouvoir distinguer au moins entre données de patients, données médicales et données non-médicales.
- Gestion des ressources informatiques (cf. **R3 : restreindre les droits d'accès et gérer les utilisateurs, R4 : sensibiliser les collaborateurs à la protection des données et, R5 : protéger les appareils contre les logiciels malveillants**)
- Gestion et échange de données (cf. **R8 : assurer des sauvegardes fiables et, R9 : assurer la sécurité des données échangées**)
- Marche à suivre lors d'incidents de sécurité (cf. **R10 : définir une procédure de gestion des incidents de sécurité**)
- Matrice d'accès et méthode d'attribution et de suppression des droits d'accès (cf. **R3 : restreindre les droits d'accès et gérer les utilisateurs**)

M-1.03 La mise en œuvre et le respect des directives de sécurité (cf. M-1.02) sont surveillés.

Vérifier si le personnel et les médecins du cabinet respectent les directives. Une check-list avec les mesures du présent document peut permettre de vérifier la mise en œuvre des directives de sécurité. Si la responsabilité informatique est confiée à un externe, les justificatifs suivants devraient être fournis au moins une fois par trimestre :

- Rapport sur les valeurs de disponibilité définies (SLA-Reporting)
- Inventaire des ressources informatiques
- Confirmation du fonctionnement de la sauvegarde et de réinitialisation des données

Si nécessaire, les justificatifs peuvent être demandés à des intervalles plus courts (par exemple confirmation quotidienne du backup ou inventaire actualisé à chaque changement).

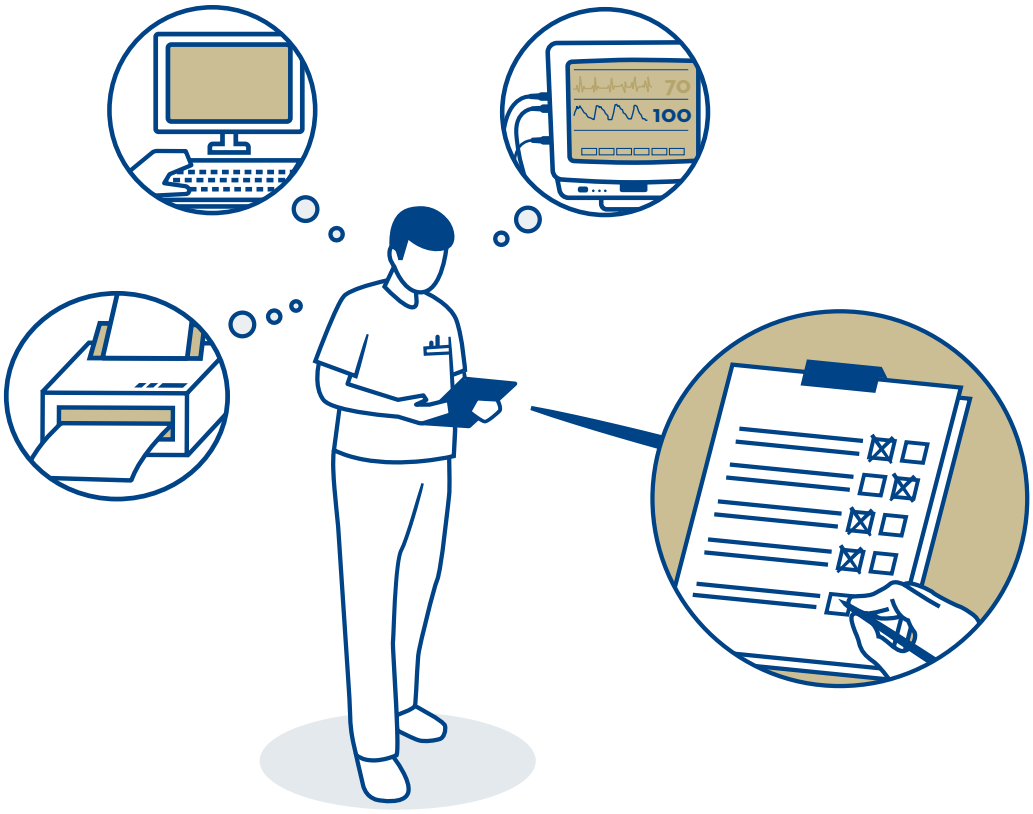
M-1.04 Il faut vérifier chaque année si les mesures de sécurité existantes peuvent être optimisées, si les exigences de sécurité (voir M-1.02) sont à jour et si les mesures techniques sont efficaces (de manière aléatoire).

Si des potentiels d'optimisation sont découverts, ils doivent être réalisés en tenant compte des avantages et des inconvénients, et les directives de sécurité existantes (voir M-1.02) doivent être adaptées.

Informations

I-1.01 OPS.1.1.3.A2 Festlegung der Zuständigkeiten – Bundesamt für Sicherheit in der Informationstechnik (en allemand)

R2
Dresser l'inventaire des ressources informatiques



Introduction

La protection efficace des données et des informations exige l'utilisation de ressources informatiques fiables. Pour cela, il faut les connaître afin de pouvoir les protéger. Cela signifie que tous les systèmes informatiques (terminaux et réseaux), tous les composants de ces systèmes (matériel informatique pour réseaux ou terminaux), tous les lecteurs de données, tous les appareils médicaux (p. ex. équipement de laboratoire, stérilisateurs, etc.) et toutes les applications doivent être identifiés, classés en fonction de la sensibilité des données et informations qu'ils traitent, et répertoriés dans un inventaire avec des attributs préalablement définis.

But

L'inventaire des ressources TIC permet d'avoir une vue d'ensemble de tout l'environnement informatique, qui englobe tout le matériel et les logiciels du cabinet. Il sert d'aide à la planification des mesures de sécurité et améliore la réactivité en cas d'incident de sécurité. Les changements, c'est-à-dire les systèmes informatiques, le matériel et les logiciels nouveaux ou mis hors service, doivent être immédiatement enregistrés. L'inventaire des ressources informatiques peut également être utilisé comme outil de planification des migrations et autres projets TIC.

Mesures

M-2.01 Toutes les ressources informatiques (cf. définition au glossaire) utilisées au cabinet ou mises à disposition par celui-ci doivent être inscrites dans un inventaire, par exemple une liste Excel, mise à jour régulièrement.

M-2.02 Toutes les ressources informatiques figurant dans l'inventaire sont répertoriées avec au moins les caractéristiques suivantes :

- Nom et désignation
- Données d'identification (p. ex n° d'identification du système)
- Utilisation
- Localisation du matériel
- Personne responsable
- Droits d'accès à cette ressource informatique
- Éléments d'adressage (DNS, adresse IP) du matériel informatique
- Indication concernant la garantie et la maintenance du matériel
- Versions logicielles utilisées (système d'exploitation, antivirus, applications)
- Date d'expiration et émetteur des certificats utilisés (certificats SSL/TLS)

M-2.03 Les nouvelles ressources informatiques sont immédiatement inscrites dans l'inventaire et celles qui ne sont plus utilisées sont supprimées. Les modifications apportées aux caractéristiques (M-2.02) sont ajoutées à l'inventaire.

L'inventaire des ressources informatiques devrait être revu et mis à jour au moins une fois par an.

M-2.04 Seules les ressources informatiques acquises par le cabinet médical sont utilisées.

M-2.05 Dans le cas de mise hors service de ressources informatiques, en particulier lorsqu'il s'agit de terminaux, toutes les données doivent être totalement effacées, et ce de manière irrévocable, immédiatement après la mise hors service de l'appareil et avant son élimination. Si le chiffrement du disque dur (M-7.02) a été effectué, les données peuvent être effacées ou écrasées par des données aléatoires. Sinon, la mesure M-7.02 doit d'abord être mise en œuvre.

Informations

I-2.01 La liste (inventaire) peut être incorporée au registre des activités de traitement.
Guide pour le registre des activités de traitement
Modèle de registre des activités de traitement

R3

Restreindre les droits d'accès et gérer les utilisateurs

Introduction

L'administration des droits d'accès des utilisateurs comprend tous les processus et toutes les applications servant à gérer les accès aux terminaux, applications et ressources. Les utilisateurs doivent s'authentifier avant de pouvoir accéder à un terminal ou à une application.

Lors de l'authentification, les utilisateurs prouvent leur identité (nom d'utilisateur). Selon la méthode d'authentification, ils saisissent une information secrète connue de l'appareil/l'application (mot de passe) ou procèdent à une vérification biométrique via les empreintes digitales, le balayage facial ou de l'œil (iris). L'appareil ou l'application vérifie ensuite l'identité de l'utilisateur, c'est ce qu'on appelle l'authentification. L'autorisation dépend des droits octroyés par le propriétaire des données.

But

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

M-3.01 L'accès aux données des patients et aux données médicales exige de configurer des comptes personnels pour chaque membre du personnel et du corps médical avec les droits d'accès requis.

Le nombre de comptes d'utilisateurs disposant de droits étendus (administrateurs, super-utilisateurs ou similaires) sur les terminaux et les applications doit être réduit au minimum.

M-3.02 Les droits d'utilisation sont limités pour les données des patients et les données médicales. Seuls les droits nécessaires pour le travail quotidien sont attribués aux utilisateurs et aux administrateurs (principe Need-to-Know).

Rôle	Données			Attribution
	Données médicales	Données des patients	Données comptables	
User	○	○	×	Assistantes médicales
Super User	○	○	○	Médecin/propriétaire du cabinet/responsable assistantes médicales
Personnel administratif	×	×	○	Back-office
Personnel technique	×	×	×	Responsable informatique

Figure 3
Exemple de matrice d'accès
○ accès illimité
× pas d'accès

Le propriétaire du cabinet décide des droits d'accès (attribution/retrait) et le responsable PSD se charge de les donner et de les supprimer.

M-3.03 Un compte personnel est utilisé pour accéder au réseau interne du cabinet via l'internet (accès VPN) avec une procédure d'authentification forte (deux facteurs indépendants, p. ex. mot de passe et jeton d'authentification).

M-3.04 Les droits d'accès sont adaptés immédiatement après chaque entrée en fonction ou chaque départ. Il est recommandé de procéder à une vérification générale chaque année.

M-3.05 Les accès à distance par des prestataires TIC externes pour des interventions de maintenance se font via des comptes d'utilisateurs personnels séparés. Les activités des comptes d'utilisateurs (tentatives de login et de logout) sont enregistrées et surveillées afin de pouvoir identifier les comportements atypiques et les retracer. Les heures d'accès à distance par un prestataire TIC externe sont communiquées à l'avance.

M-3.06 Tous les mots de passe doivent être changés à intervalles réguliers. Dans la mesure du possible, ce changement (par exemple pour les comptes d'utilisateurs) est imposé techniquement par l'attribution d'une durée de validité limitée. Si ce n'est pas possible, le cabinet met en place l'organisation requise pour assurer le changement régulier des mots de passe.

M-3.07 Les mots de passe et les codes PIN utilisés doivent présenter les caractéristiques suivantes :

- Minimum 10 caractères,
- Des chiffres, des lettres majuscules et minuscules ainsi que des caractères spéciaux,
- Pas de combinaisons en séquences ni de lettres voisines sur le clavier comme asdfgh ou 45678,
- Pas de mot pouvant se trouver dans un dictionnaire (dans toutes les langues), ni de nom, prénom, date de naissance ou localité ; le mot de passe ne doit avoir aucune signification,
- Un seul compte par mot de passe,
- Confidentialité et
- Utilisation exclusive au cabinet médical et jamais pour des services privés.

M-3.08 Si la biométrie, comme les empreintes digitales ou la reconnaissance faciale, est utilisée sur les appareils mis à disposition par le cabinet, il est important de veiller à toujours ajouter un code PIN ou un mot de passe pour que tout appareil ait deux possibilités de dé-/verrouillage (cf. **R3 : restreindre les droits d'accès et gérer les utilisateurs**).

M-3.09 Les mots de passe sont archivés dans un programme de gestion des mots de passe et mis à la disposition des personnes compétentes.

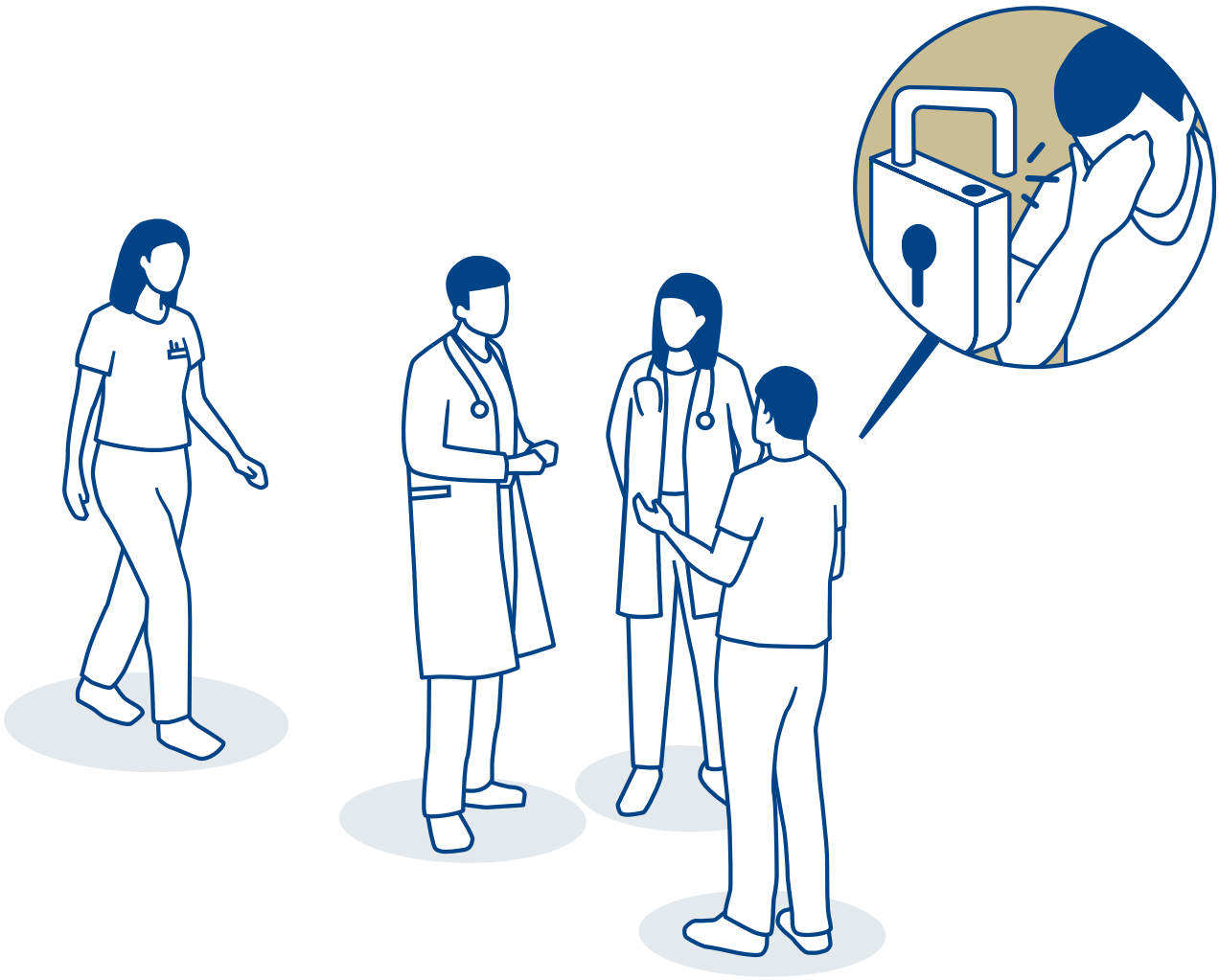
M-3.10 Les utilisateurs verrouillent les appareils lorsqu'ils quittent leur lieu ou poste de travail ou se déconnectent de leur compte.

Informations

I-3.01 Check-list : mots de passe sécurisés – HIN

R4

Sensibiliser les collaborateurs à la protection des données



Introduction

Les membres du personnel et du corps médical sont sensibilisés à la protection et à la sécurité des données, ils se familiarisent avec les directives et instructions à suivre en cas d'incidents de sécurité. La sensibilisation peut se faire par différents moyens : formation, fiche d'information, communication ciblée ou formation continue.

But

Les pirates informatiques 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, le personnel et les médecins du cabinet.

La sensibilisation permet d'attirer l'attention sur les attaques/objectifs d'attaque possibles, d'encourager une utilisation sûre des ressources informatiques et de faire attention lors du traitement de données sensibles.

Mesures

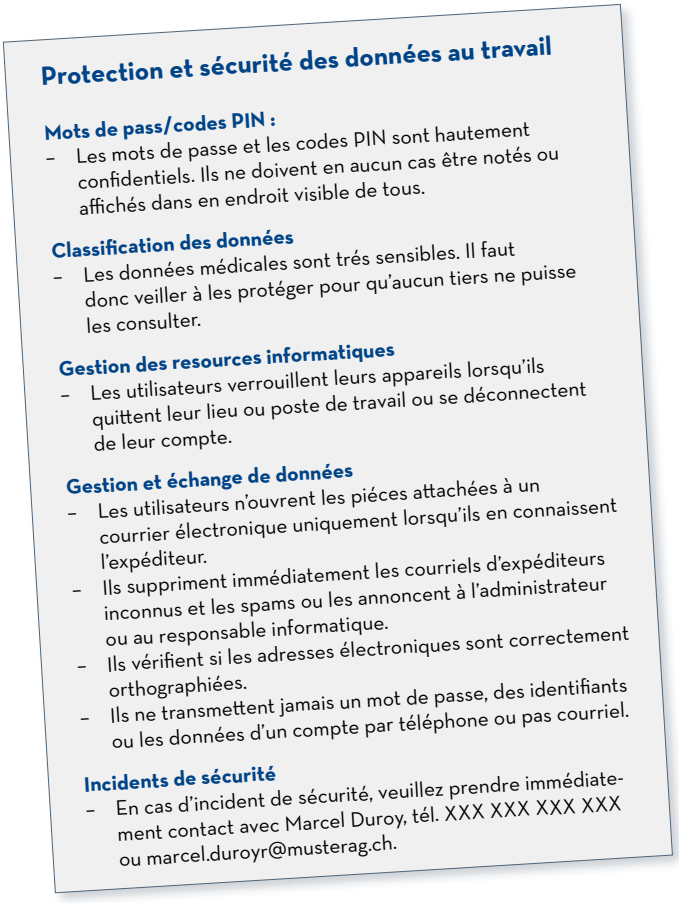
M-4.01 Les dates, thèmes abordés et canaux de communication utilisés sont définis en vue de sensibiliser le responsable et le personnel du cabinet aux questions de la sécurité informatique. Cette sensibilisation cible au moins les consignes de sécurité de la mesure M-1.02 (cf. **R1 : définir les responsabilités et fixer les directives informatiques**).

- Dangers
- Mots de passe et codes PIN
- Classification des données et gestion des différentes classifications
- Gestion des ressources informatiques
- Gestion et échange de données
- Marche à suivre lors d'incidents de sécurité

M-4.02 Au moment de l'entrée en fonction et ensuite régulièrement, les membres du personnel et du corps médical sont sensibilisés aux questions soulevées par la mesure M-4.01, ce qui les encourage à être durablement attentifs à la protection, à la sécurité et à une gestion raisonnée des données. Les nouveaux membres du personnel suivent les formations et signent une déclaration de consentement confirmant qu'ils comprennent et respectent les consignes de sécurité informatique du cabinet. Les membres du personnel qui quittent leur fonction sont également sensibilisés à l'obligation de conserver le secret après leur départ de l'entreprise.

M-4.03 Le domaine de la protection et de la sécurité des données, en particulier les points mentionnés dans le mesure M-4.01 est abordé au moins deux fois par an, par exemple lors de réunions d'équipe.

M-4.04 Une notice proposant des conseils relatifs à la mesure M-4.01 est distribuée aux employés et placé à des endroits bien en vue (poste de travail/téléphone). Voici un exemple :



Protection et sécurité des données au travail

Mots de pass/codes PIN :
- Les mots de passe et les codes PIN sont hautement confidentiels. Ils ne doivent en aucun cas être notés ou affichés dans en endroit visible de tous.

Classification des données
- Les données médicales sont trés sensibles. Il faut donc veiller à les protéger pour qu'aucun tiers ne puisse les consulter.

Gestion des resources informatiques
- Les utilisateurs verrouillent leurs appareils lorsqu'ils quittent leur lieu ou poste de travail ou se déconnectent de leur compte.

Gestion et échange de données
- Les utilisateurs n'ouvrent les piéces attachées à un courrier électronique uniquement lorsqu'ils en connaissent l'expéditeur.
- Ils suppriment immédiatement les courriels d'expéditeurs inconnus et les spams ou les annoncent à l'administrateur ou au responsable informatique.
- Ils vérifient si les adresses électroniques sont correctement orthographiées.
- Ils ne transmettent jamais un mot de passe, des identifiants ou les données d'un compte par téléphone ou pas courriel.

Incidents de sécurité
- En cas d'incident de sécurité, veuillez prendre immédiatement contact avec Marcel Duroy, tél. XXX XXX XXX XXX ou marcel.duroyr@musterag.ch.

Figure 4
Exemple de notice

M-4.05 Tous les membres du personnel sont informés des événements importants pour la sécurité, de leurs conséquences et des adaptations éventuelles des consignes de sécurité (cf. M-1.02) et ce dans les meilleurs délais, par exemple lors des réunions d'équipe.

M-4.06 Les pièces jointes aux courriels peuvent contenir des logiciels malveillants. Si l'expéditeur est inconnu, le courriel est supprimé sans avoir ouvert le ou les documents joints.

Les courriels d'hameçonnage ou les spams sont supprimés sans avoir cliqué sur les liens ou les pièces jointes et sans y avoir répondu.

En cas de doute sur la provenance d'un courriel d'hameçonnage ou d'un spam, il est recommandé de s'adresser au responsable PSD.

M-4.07 L'utilisation à titre privé des ressources informatiques mises à disposition par le cabinet est clairement réglementée. Elle ne devrait pas être possible s'il s'agit d'accéder à des données sensibles.

Les appareils utilisés à la fois à des fins professionnelles et privées sont dotés de deux comptes d'utilisateur pour empêcher l'accès aux données professionnelles à partir du compte privé.

L'accès à internet à des fins privées (messagerie privée ou navigation sur internet) en utilisant les appareils du cabinet est à éviter ou à réduire au minimum. Cette restriction peut être mise en œuvre techniquement en définissant une liste des pages internet relevant des affaires du cabinet (whitelisting).

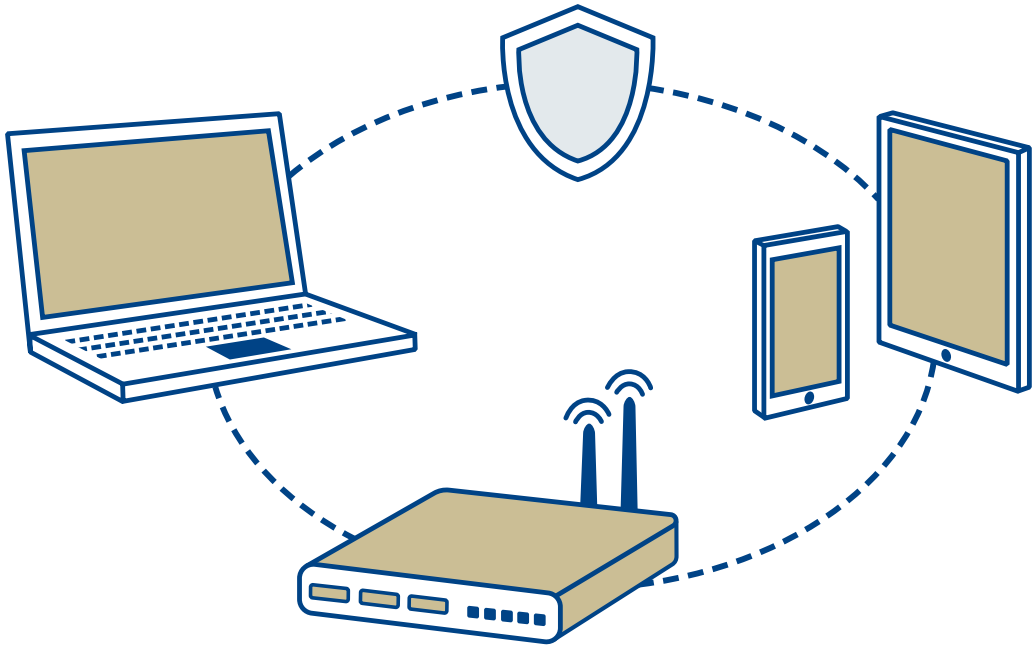
Informations

I-4.01 Thèmes actuels – Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI)

I-4.02 Awareness Portal – HIN

R5

Protéger les appareils contre les logiciels malveillants



Introduction

Les logiciels malveillants sont des programmes informatiques créés dans le but de voler, de manipuler ou de détruire des données sur des appareils distants. En fonction de l'objectif poursuivi, ils sont appelés communément virus, ver informatique ou cheval de Troie (de chiffrement). Ils se propagent via des pièces jointes, des liens vers des sites internet ou des supports de données tels que des clés USB.

But

Les appareils comme les téléphones ou les ordinateurs portables peuvent être facilement infectés par un logiciel malveillant. Il est indispensable d'installer un programme de protection antivirus pour réduire ce risque et de le configurer de sorte que toutes les données soient vérifiées avant ouverture et les logiciels malveillants détectés selon des modèles connus pour bloquer leur exécution. Ces mesures permettent de réduire considérablement les risques mais il est important de souligner que les programmes antivirus ne reconnaissent que les maliciels connus. Une protection complète n'est pas garantie. Il est donc essentiel de sensibiliser aux dangers potentiels notamment lors du traitement des courriels, des liens dans les e-mails et des fichiers joints (R4 : sensibiliser les collaborateurs à la protection des données).

Mesures

M-5.01 Tous les ordinateurs sont équipés d'un programme de protection antivirus installé, actualisé et configuré de manière à ce que toutes les données soient vérifiées et que les mises à jour de l'antivirus soient possibles au moins une fois par jour. Les utilisateurs n'ont pas la possibilité de désactiver le programme antivirus.

Lorsque Windows Defender est le programme antivirus utilisé sur le système d'exploitation Windows 10, la protection Ransomware peut être activée comme fonction de sécurité supplémentaire.

M-5.02 Le programme de protection antivirus effectue un scan complet (full scan) une fois par semaine sur les ordinateurs. Si une alerte est déclenchée, elle est immédiatement signalée au responsable PSD ou au responsable informatique. Si possible, une annonce automatique est envoyée au service compétent.

M-5.03 Le système d'exploitation le plus récent est installé sur les ordinateurs raccordés au réseau mis à disposition par le cabinet (cf. M-7.01). Il est possible d'accorder des exceptions si les mises à jour de sécurité sont fournies pour le système d'exploitation. Tout programme ou toute application est obtenu exclusivement auprès du fabricant ou des magasins en ligne officiels.

M-5.04 Lors de l'utilisation des clés USB, il faut veiller à ce qu'aucune clé USB privée, inconnue, trouvée ou déjà utilisée ailleurs ne soit connectée aux appareils du cabinet.

M-5.05 Les ordinateurs du cabinet ne sont pas utilisés à des fins personnelles. Une telle utilisation peut être autorisée si deux comptes d'utilisateur distincts ont été mis en place, l'un pour les affaires privées et l'autre pour les affaires professionnelles (cf. M-4.07). Pour naviguer sur internet, il faut tenir compte des mesures de la **R4 : sensibiliser les collaborateurs à la protection des données**.

M-5.06 Les ordinateurs sont équipés d'une protection d'accès, c'est-à-dire d'un mot de passe (cf. les exigences de la **R3 : restreindre les droits d'accès et gérer les utilisateurs**).

M-5.07 Les terminaux qui ne répondent pas aux mesures recommandées (M-5.01 à M-5.03) ne devraient pas être raccordés aux ordinateurs du cabinet ou au réseau.

Informations

I-5.01 Logiciels malveillants : que faire contre les virus, les chevaux de Troie et les vers – HIN

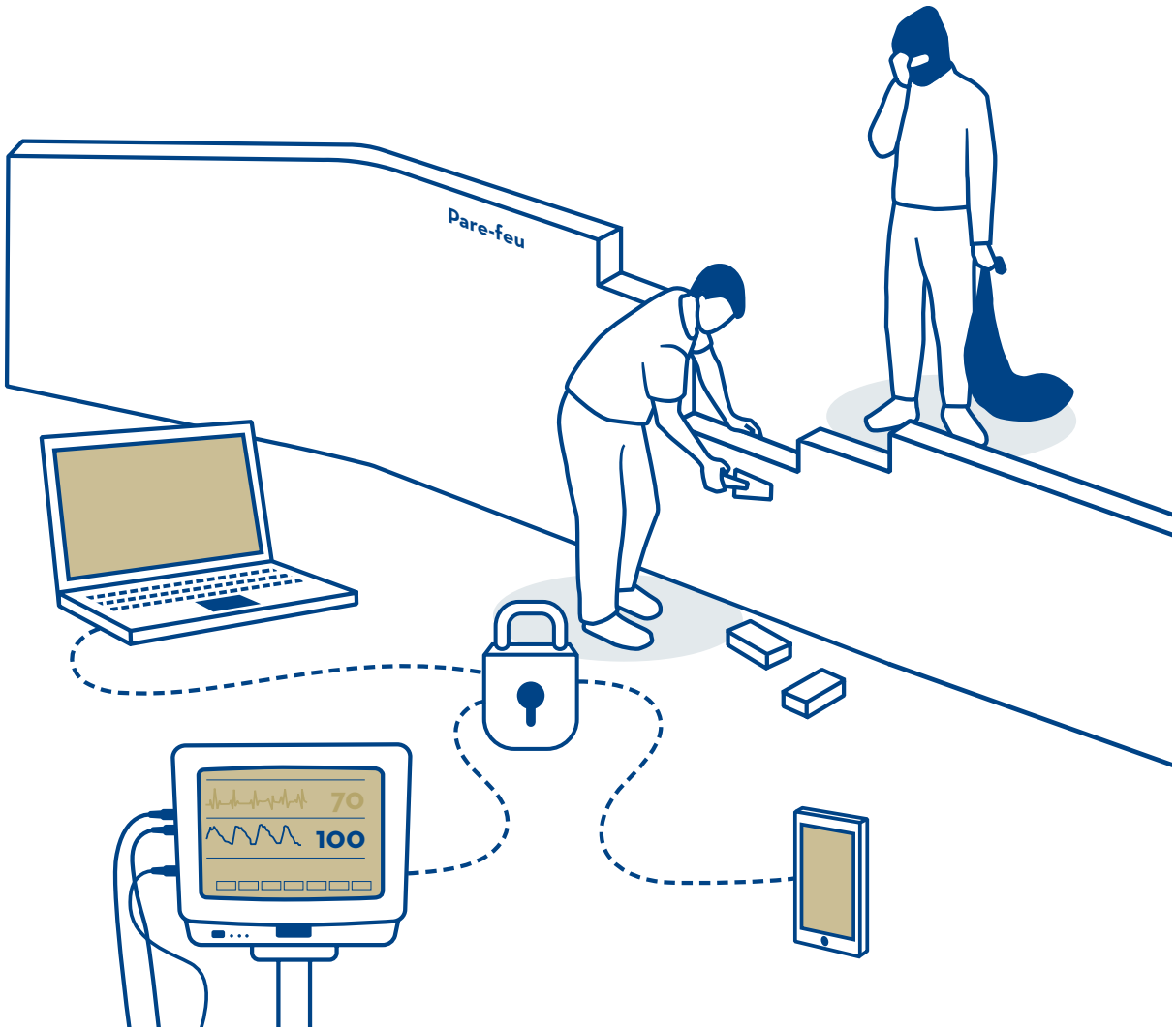
I-5.02 Endpoint Security – HIN

I-5.03 Activer l'accès contrôlé aux dossiers – Microsoft

I-5.04 Forum aux questions sur la protection anti-courrier indésirable – Microsoft

I-5.05 Questions fréquentes sur les virus, les autres logiciels malveillants et les pourriels – HIN

R6
Protéger le réseau



Introduction

Si l'accès au réseau informatique d'un cabinet médical n'est pas suffisamment protégé, le risque existe que des personnes tierces non autorisées (hacker) puissent y accéder et donc espionner la communication ou voler des données. Les prises physiques qui permettent de raccorder le câble directement à un routeur ou à une prise réseau mural et les connexions sans fil (WiFi/WLAN) sont des interfaces avec le réseau. Dans la mesure du possible, le réseau informatique du cabinet est protégé de l'internet. Seuls les raccordements nécessaires sont autorisés.

But

Afin de protéger le réseau du cabinet contre les accès non autorisés, il est important de prendre plusieurs précautions de sécurité au moment de le mettre en place, notamment au niveau de l'interface avec internet et des raccordements au réseau local, qu'ils soient avec ou sans fil.

Mesures

M-6.01 Pour empêcher les accès non autorisés au réseau du cabinet, des mesures de sécurité sont prises au niveau des interfaces avec internet (points de transition entre le réseau du cabinet et l'internet). Cela signifie que le réseau est protégé par un pare-feu. Seuls les raccordements nécessaires au fonctionnement sont autorisés. Une restriction est également recommandée pour les connexions sortantes. Lors de la sélection d'un produit, il convient de veiller à ce que le pare-feu dispose de fonctionnalités de sécurité supplémentaires telles que les antivirus au niveau du réseau, la détection/prévention des attaques et les filtres anti-spam pour les e-mails entrants, si un tel filtre n'est pas déjà intégré dans le serveur mail.
Il faut vérifier au moins une fois par trimestre si des mises à jour existent. De plus, les règles du pare-feu doivent être vérifiées au moins une fois par an et ajustées si nécessaire.

M-6.02 L'accès au réseau du cabinet par une connexion sans fil ne doit être mis en place qu'en cas de besoin absolu. Si une connexion WiFi est utilisée, l'accès doit être protégé par un mot de passe (cf. **R3 : restreindre les droits d'accès et gérer les utilisateurs**) et mis uniquement à la disposition d'utilisateurs autorisés. Le mot de passe est changé chaque année.

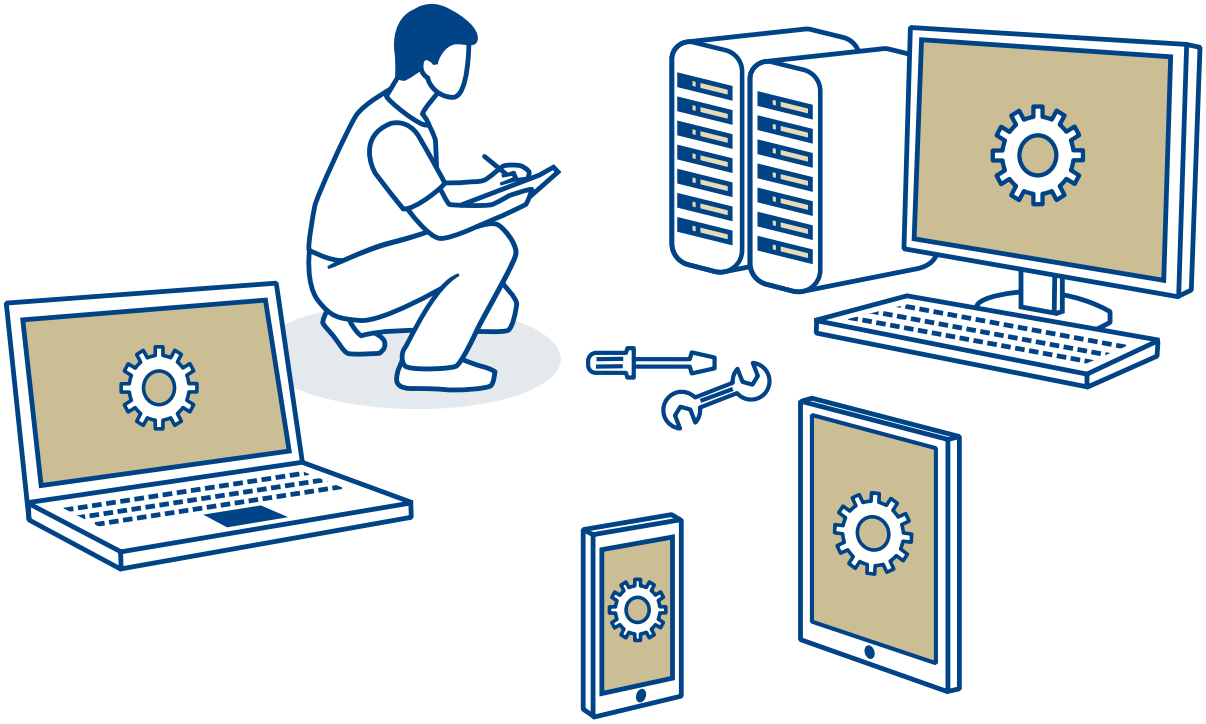
M-6.03 Les prises réseau non utilisées sont condamnées et n'ont aucun raccordement avec le réseau, sinon des personnes non autorisées pourraient s'y connecter. C'est particulièrement important dans les endroits accessibles au public comme les salles d'attente.

M-6.04 Lorsqu'une infrastructure informatique est plus importante et qu'elle est exploitée avec plusieurs serveurs, ou si un WLAN est proposé aux invités, le réseau doit être divisé ou « segmenté » en plusieurs parties. Cela permet de garantir que les utilisateurs du réseau WLAN public n'ont pas accès au réseau interne.
L'accès au réseau WLAN public est protégé par un mot de passe.

Informations

I-6.01 NET.3.1.A1 Sichere Grundkonfiguration eines Routers oder Switches – Bundesamt für Sicherheit in der Informationstechnik (en allemand)

R7
Configurer et entretenir l'infrastructure informatique



Introduction

La configuration efficace des systèmes et des éléments du réseau permet de réduire la surface d'attaque et donc aussi la probabilité et l'impact d'une cyberattaque. La réalisation de ces configurations de sécurité s'appelle le durcissement informatique. Ce durcissement est à mettre en place avant l'utilisation effective du réseau. En raison d'obstacles techniques ou contractuels, il peut être difficile voire impossible d'intervenir sur des systèmes informatiques (p. ex. les appareils de laboratoire) qui sont entièrement livrés par un prestataire externe. Ce genre de systèmes doivent donc faire l'objet d'un traitement particulier, et par exemple être placés dans une zone du réseau qui leur est réservée, car sur la plupart, aucune possibilité de mise à jour n'est installée ou il est impossible de procéder à leur durcissement.

But

En durcissant la configuration des systèmes informatiques et des composants réseau, il est possible de réduire la surface d'attaque et donc aussi la probabilité et l'impact d'une attaque informatique.

Mesures

M-7.01 Les systèmes informatiques, en particulier les ordinateurs, les ordinateurs portables et les smartphones, ainsi que les composants réseau, sont configurés de manière à permettre l'installation rapide et automatique des mises à jour des systèmes d'exploitation et des applications installées, ainsi que des mises à jour de sécurité.

Les systèmes informatiques et les applications qui ne sont plus pris en charge par le fabricant ne sont pas adaptés à une utilisation dans un environnement sensible et doivent donc être remplacés. Des exceptions sont possibles si des mises à jour de sécurité de l'application et des systèmes informatiques sont fournis par le fabricant.

M-7.02 Les systèmes informatiques doivent être renforcés autant que possible par les mesures de durcissement informatique suivantes :

- Les logiciels, outils et comptes utilisateurs inutiles sont supprimés des systèmes.
- Les comptes utilisateurs sont personnels et n'ont que les droits d'accès requis pour le travail. Le compte administrateur impersonnel n'est utilisé qu'une fois pour la création des comptes administrateurs personnels. Le compte utilisateur invité est désactivé.
- Tous les comptes utilisateurs, en particulier ceux qui ont des droits d'accès plus étendus, sont dotés d'un mot de passe sécurisé (cf. **R3 : restreindre les droits d'accès et gérer les utilisateurs**).
- Le chiffrement du disque dur est activé pour qu'une personne ayant un accès direct au disque dur, par exemple après un vol, n'ait pas accès aux données elles-mêmes.
- Le BIOS, qui se charge du démarrage du système d'exploitation, est sécurisé par un mot de passe. En outre, le BIOS est configuré de sorte qu'il n'est pas possible de démarrer un système d'exploitation à partir d'un support amovible.
- Le démarrage automatique des lecteurs externes tels que le lecteur de CD est désactivé.
- L'indication de l'heure est synchronisée sur tous les systèmes.
- Le serveur de messagerie est configuré pour analyser les pièces jointes, détecter d'éventuels programmes malveillants et bloquer les pièces jointes dont l'extension de fichier correspond à celles typiquement utilisées pour envoyer des programmes malveillants, à savoir : .JS, .JSE, .BAT, .PIF, .VBS, .LNK, .EXE, .REG, .CMD, .SCR, .DOCM (document Word avec des macros)

M-7.03 Il est préférable de déplacer les systèmes informatiques ayant peu ou pas du tout de possibilités de configuration, comme les appareils médicaux (appareils de laboratoire, stérilisateurs, etc.) dans une zone du réseau qui leur est dédiée ou de les déconnecter entièrement du réseau (cf. **R6 : protéger le réseau**). Cette zone dédiée aux appareils médicaux est configurée de telle sorte que seules les connexions entrantes et sortantes nécessaires au fonctionnement sont possibles.

M-7.04 Dans la mesure du possible, les systèmes informatiques et les applications sont configurés de telle sorte que les activités liées à la sécurité, telles que les tentatives de login, les connexions (login), les déconnexions (logout), les mutations, les plantages de données, de systèmes ou d'applications, sont enregistrées.

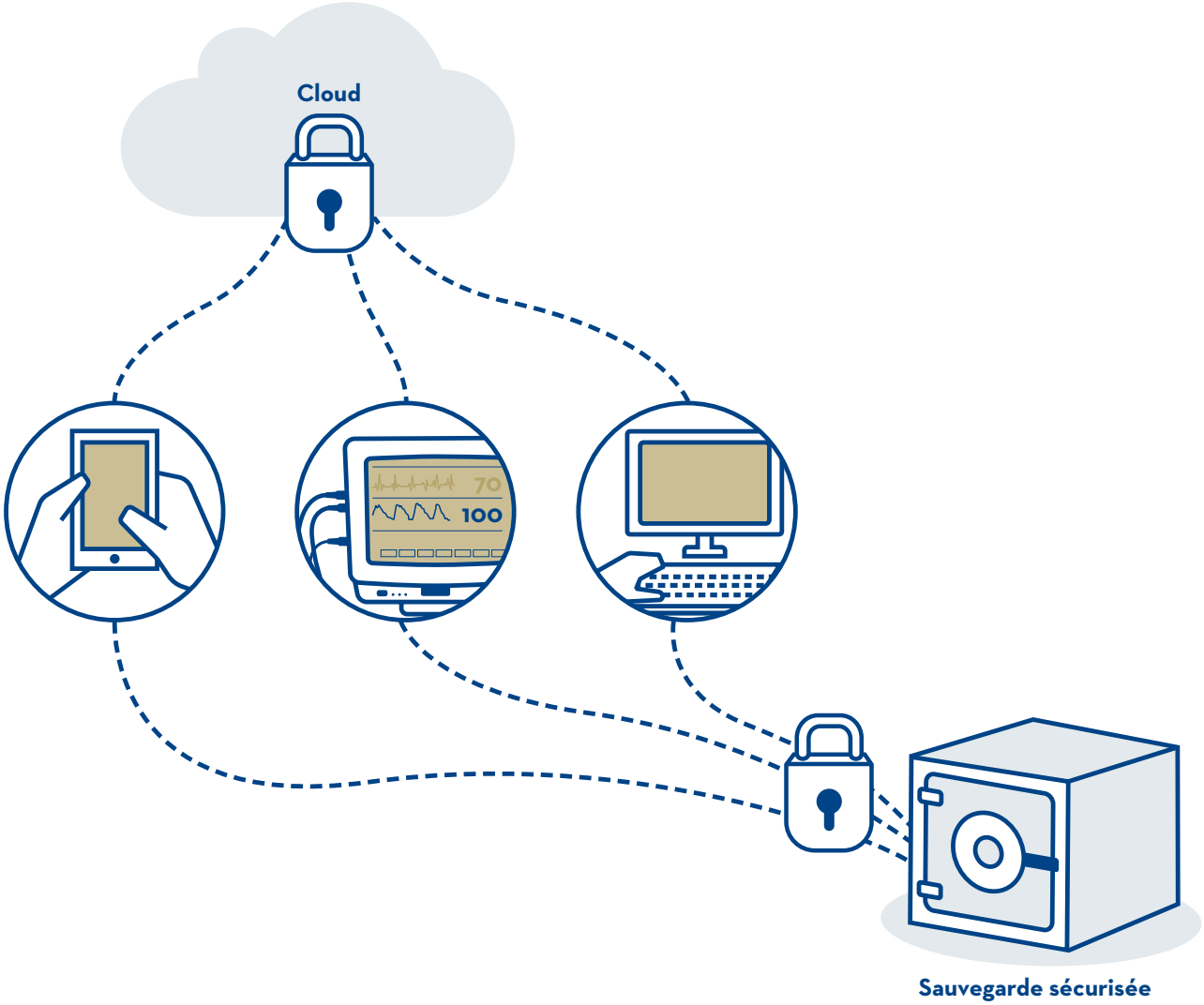
Les journaux sont conservés de manière centralisée et ne peuvent être consultés qu'avec des droits d'accès limités.

Les données du journal sont conservées pendant au moins trois mois et, si nécessaire, rendues accessibles à des fins d'évaluation (par exemple, en cas de suspicion d'un incident de sécurité).

M-7.05 Pour la surveillance opérationnelle, il est recommandé que les systèmes informatiques et les applications utilisés enregistrent et analysent les activités des utilisateurs et, en cas de mise hors service d'un système, envoient une notification.

M-7.06 Il est recommandé de disposer d'une garantie du fabricant indiquant les échéances de remplacement définies pour les appareils essentiels au fonctionnement ou d'avoir à portée de main des appareils de remplacement équivalents.

R8
Assurer des sauvegardes fiables



Introduction

Les données stockées sur les systèmes informatiques ou les lecteurs de données peuvent être supprimées accidentellement ou par du matériel défectueux ou un logiciel malveillant. Des droits d'accès trop étendus ou des données non chiffrées peuvent compromettre la confidentialité, l'intégrité et la disponibilité des données.

But

Pour éviter le risque de perdre des données, il est important de procéder régulièrement à des sauvegardes. Afin d'assurer la confidentialité et l'intégrité des données sauvegardées, il est important de leur attribuer des droits d'accès et d'utilisation pour les protéger de la même manière que les données initiales.

Recommandation 8

Mesures

M-8.01 Il est nécessaire de déterminer quelles données sont intégrées dans la sauvegarde et à quelle fréquence elles sont sauvegardées. Au moins, une copie de sauvegarde doit être conservée à l'extérieur du cabinet.

M-8.02 La sauvegarde est stockée hors du cabinet ; l'archivage des sauvegardes est documenté afin d'avoir trace de toutes les données sauvegardées.

M-8.03 Le logiciel de sauvegarde utilisé est configuré comme suit :

- Les sauvegardes sont archivées sous forme chiffrée.
- Le mot de passe du chiffrement n'est connu que du propriétaire du cabinet et stocké dans un coffre-fort ou un casier.
- Le cabinet procède à au moins une sauvegarde incrémentielle quotidienne et au moins à une sauvegarde complète par semaine. Les sauvegardes sont stockées sur un support de données séparé ou sur un dispositif de stockage externalisé (par ex. service sur le cloud). La sauvegarde incrémentielle enregistre les données qui ont changé depuis la dernière sauvegarde, par exemple, la sauvegarde du mardi ne contient que les données qui ont changé depuis lundi.
- Il est recommandé de procéder au versionnage des fichiers afin de pouvoir consulter des versions antérieures des documents.
- Les droits d'accès aux fichiers de la sauvegarde sont maintenus et équivalents aux droits originaux.
- Les disques locaux sont changés tous les jours pour empêcher l'accès aux logiciels malveillants, mais aussi pour éviter les dommages physiques.
- Les données sauvegardées sont déplacées au moins une fois par semaine dans un endroit externe et sécurisé, par exemple dans une pièce verrouillée à l'extérieur du cabinet.

M-8.04 La réinitialisation des données de la sauvegarde est testée au moins une fois par an.

M-8.05 La sécurisation des données primaires ou des sauvegardes dans le cloud obéit à des règles strictes. Par ailleurs, les exigences de la loi sur la protection des données et l'obligation de confidentialité doivent être respectées. Sont exclusivement admis les fournisseurs qui remplissent les « Exigences techniques et organisationnelles pour les services sur le cloud » définies par la FMH.

Lorsque le cabinet utilise une solution sur le cloud, le patient doit en être informé tout comme il est informé des données recueillies et de leur utilisation.

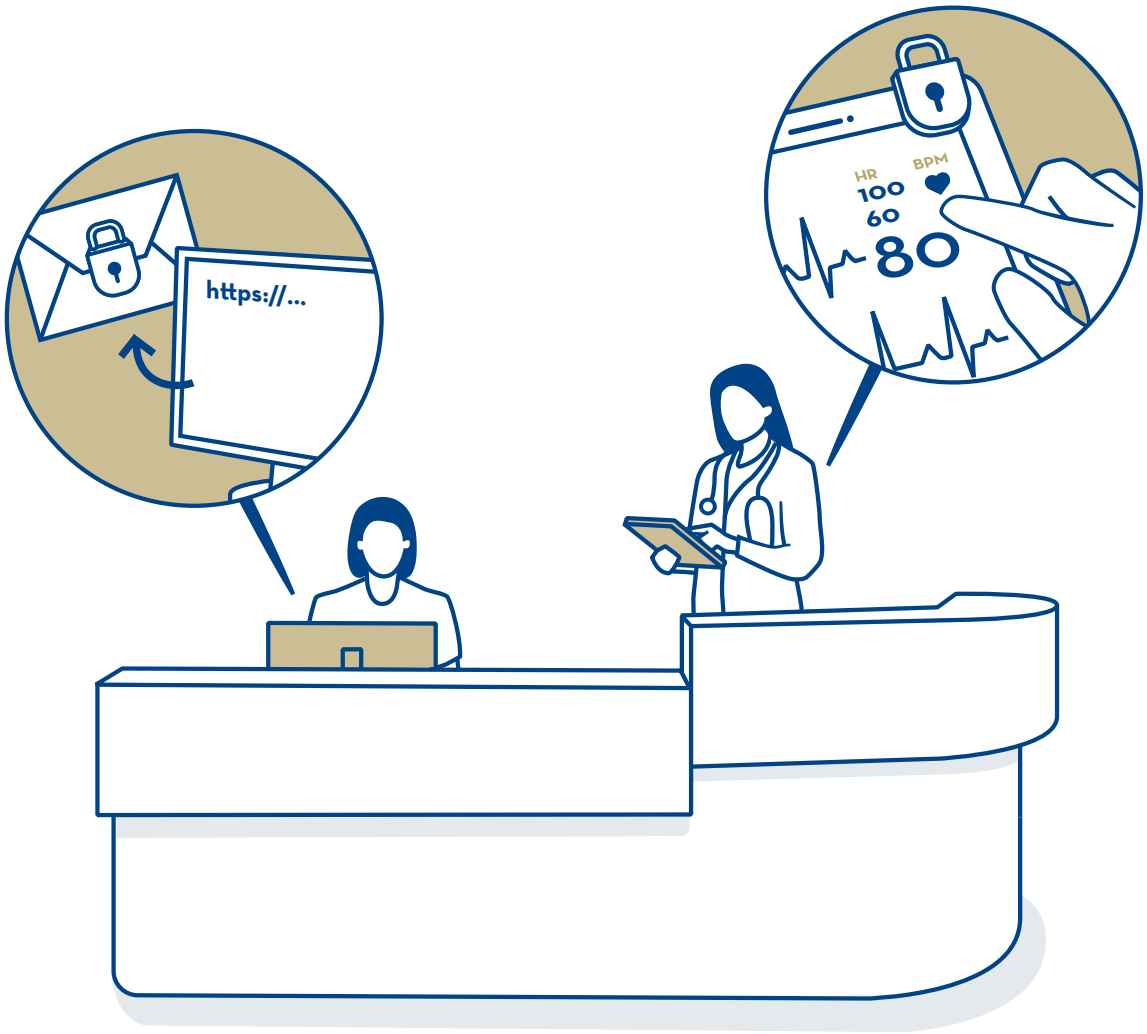
Informations

I-8.01 Conservation de dossiers médicaux dans le nuage – Préposé fédéral à la protection des données et à la transparence (PFPDT)

I-8.02 Contrat-cadre de la FMH pour les services sur le cloud

I-8.03 Exigences techniques et organisationnelles pour les services sur le cloud – FMH

R9
Assurer la sécurité des données échangées



Introduction

Les données sensibles doivent être protégées par chiffrement pour éviter tout accès par des personnes non autorisées. Cela permet de garantir que les données échangées par e-mail, fax ou message instantané ne peuvent être consultées, supprimées ou modifiées que par des personnes autorisées. Cela permet aussi d'empêcher que des données soient modifiées sans que personne ne s'en rende compte.

But

Le chiffrement permet de protéger les informations, les données et la communication en empêchant qu'elles puissent être consultées et manipulées. Les échanges sécurisés servent à garantir la confidentialité, l'authenticité du message et de l'expéditeur.

La confidentialité d'un message est protégée par le chiffrement et le fait qu'une seule personne possède la clé pour le déchiffrer.

L'utilisation du chiffrement permet de voir si des modifications ont été apportées à un message, et garantit l'impossibilité de modifier un message chiffré.

L'authenticité peut être vérifiée par une signature numérique, puisque seul l'expéditeur possède la clé de signature correspondante.

Mesures

M-9.01 L'accès aux applications via internet doit se faire uniquement par une connexion sécurisée (par ex. HTTPS). Les données des patients, les données médicales et les caractéristiques d'authentification, comme les mots de passe, ne doivent pas être transmises sans chiffrement.

M-9.02 Les données des patients et les données médicales sont chiffrées pour les échanges par e-mail. Pour cela, il faut choisir une solution de chiffrement utilisée pour la communication entre les acteurs du secteur de la santé. Les produits HIN peuvent être utilisés à cette fin, par exemple.

M-9.03 Dans la mesure du possible, les appels téléphoniques doivent être identifiés avant de donner des renseignements sur les données médicales et les données des patients afin d'écarter toute possibilité d'une attaque d'ingénierie sociale.

M-9.04 Les télécopies ne sont pas transmises sous forme chiffrée et doivent donc être réduites au minimum. Les télécopieurs doivent être placés de façon à ce que les messages entrants ne puissent pas être lus par des personnes non autorisées.

M-9.05 Tous les processus liés aux ordres de paiement sont clairement réglementés au sein du cabinet et respectés par tous les collaborateurs ; par exemple double contrôle et signature collective, ce qui signifie qu'avant d'être validés, les versements, sont visés par un autre utilisateur du eBanking. Cela s'applique particulièrement aux cabinets dans lesquels plusieurs membres du personnel sont habilités à faire des versements.

Informations

I-9.01 Mail : une communication sécurisée entre abonnés – HIN

R10

Définir une procédure de gestion des incidents de sécurité

Introduction

Les incidents de sécurité sont des événements qui affectent la confidentialité, l'intégrité et la disponibilité des informations et des données. Les attaques de phishing, l'exploitation des points faibles d'un système, l'infection par un logiciel malveillant (virus, vers informatiques ou chevaux de Troie) l'accès non autorisé à des clés de chiffrement sont des exemples d'incidents pouvant avoir un impact considérable sur le fonctionnement d'un cabinet médical.

Les incidents de sécurité peuvent survenir dans le domaine de la sécurité physique, de l'environnement informatique, des groupes d'utilisateurs et de parties prenantes ainsi que sur des applications et des terminaux.

En fonction de l'incident, l'infrastructure informatique devra peut-être être restaurée pour pouvoir reprendre ses activités. La procédure de base, les responsabilités dans un tel cas ainsi que les coordonnées des personnes et des entreprises impliquées doivent être définies à l'avance et mises à la disposition du personnel du cabinet, des médecins et du responsable.

But

Des mesures adéquates dans les domaines de la technologie, de l'infrastructure et du personnel peuvent protéger de manière préventive les cabinets médicaux contre les événements néfastes. Cependant, il n'est pas possible de réduire complètement les risques. Il est primordial de définir les procédures organisationnelles et techniques, et les aides spécifiques utilisées pour la détection et le traitement rapides et efficaces des incidents de sécurité. L'objectif est de limiter autant que possible l'étendue des dégâts.

Mesures

M-10.01 L'interlocuteur chargé de signaler les incidents de sécurité et son remplaçant sont désignés. Leurs coordonnées et disponibilités sont communiquées au responsable et aux membres du personnel et du corps médical.

M-10.02 Les notices spécifiant la marche à suivre en cas d'incidents de sécurité ou la post-analyse existent et sont mis à la disposition des membres du personnel et des médecins. Elles abordent au moins les quatre thèmes suivants :
- Définition et exemples d'incidents de sécurité
- Check-list pour l'annonce, l'analyse et le traitement d'incidents (instructions sur la manière d'agir)
- Coordonnées des personnes à informer
- Directives pour la communication interne et externe
- Marche à suivre avec les autorités de poursuite pénale

M-10.03 Pour l'analyse d'un incident de sécurité, il faut au moins répondre aux questions suivantes (check-list pour l'analyse d'un incident de sécurité) :
- Quels sont les éléments concernés par l'incident de sécurité ?
- Qui l'a remarqué et signalé ?
- Quel groupe d'utilisateurs/quelles données sont concernées (taille, criticité, etc.) ?
- Quels éléments supplémentaires pourraient être touchés ?
- Qu'est-ce qui l'a déclenché (négligence, attaque, défaillance de l'infrastructure de sécurité, etc.) ?
- Seuls des personnes internes sont concernées ou aussi des patients ?

M-10.04 Suite à un incident de sécurité, des mesures immédiates telles que l'isolement ou la mise hors service de certains services ou terminaux sont prises en cas de vol ou d'effacement de données médicales ou de données de patients. Toute violation de la sécurité des données doit être signalée le plus rapidement possible au Préposé fédéral à la protection des données et à la transparence (PFPDT) pour autant qu'elle présente un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée.

M-10.05 En cas de soupçon de délit, il est primordial de prendre très rapidement contact avec la police, afin d'agir avant la disparition de traces éventuelles. La police apporte conseil et soutien, notamment pour répondre aux questions en lien avec le versement ou non d'une rançon. Les attaques sans dommage peuvent être annoncées au Centre national pour la cybersécurité NCSC.

M-10.06 Toutes les personnes que l'incident expose à un risque élevé au niveau de leurs droits fondamentaux et de la personnalité sont informées dans les meilleurs délais.

M-10.07 Les conclusions tirées après un incident de sécurité sont communiquées rapidement au personnel, par exemple lors des réunions d'équipe. Si le PFPDT ou les personnes concernées doivent être informés conformément à M-10.04 et/ou M-10.06, le personnel doit alors aussi être informé de l'incident.

M-10.08 Les conclusions tirées après un incident de sécurité sont intégrées aux mesures de sécurité internes de M-1.02 et les changements sont communiqués. Par exemple, la procédure lors d'incidents de sécurité est adaptée si le potentiel d'optimisation permet une gestion plus efficace des incidents de sécurité.

Informations

I-10.01 M 6.130 Erkennen und Erfassen von Sicherheitsvorfällen – Bundesamt für Sicherheit in der Informationstechnik (en allemand)

I-10.02 Site internet du Préposé fédéral à la protection des données et à la transparence pour signaler les violations de la sécurité des données

I-10.03 Formulaire d'annonce au Centre national pour la cybersécurité (NCSC)

I-10.04 Cybercrime – Matériel d'information pour les PME, police cantonale bernoise

I-10.05 Liste de contrôle et déroulement de la procédure en cas de violation de la protection des données – FMH

R11

Mandater des prestataires externes et superviser leur travail

Introduction

Selon l'accord contractuel, les prestataires de services externes sont responsables de la mise en place, de l'exploitation, de l'entretien et de la maintenance de l'environnement informatique. Le choix de l'offre la mieux adaptée nécessite une étude approfondie du marché, notamment avant l'achat de services sur le cloud.

But

L'évaluation des prestataires permet de trouver un fournisseur qui répond aux exigences requises en matière de protection et de sécurité des données.

Les aspects suivants doivent être vérifiés :

- Les critères souhaités sont-ils remplis ?
- Les transferts de données et les attributions de tâches sont-ils dotés d'une restriction concernant le secret médical et la protection des données ?
- Les tâches demandées sont-elles au cœur du modèle d'affaires ?
- Le traitement et le stockage des données se font-ils en Suisse ?
- Quel est le droit applicable et le for juridique ?
- Quelles sont les références ?
- Possibilité d'évaluations indépendantes par des tiers

Mesures

M-11.01 Le contrat de prestations avec des prestataires TIC externes est soumis aux Conditions générales pour les prestations TIC, édition de janvier 2020, de l'Administration numérique suisse; en outre, le contrat de prestations dans le domaine de la protection et de la sécurité des données doit couvrir au moins les critères suivants :

- Le traitement et le stockage des données se font selon les directives et les attentes du cabinet et sont documentés.
- Les exigences légales et réglementaires, notamment en ce qui concerne la LPD et le secret médical sont respectées.
- Le cabinet donne son soutien pour que les exigences réglementaires puissent être respectées.
- Les personnes en charge du traitement des données sont tenues au secret professionnel.
- Les incidents de sécurité présentant un risque pour les personnes concernées ou le cabinet médical sont annoncés immédiatement.
- Les sous-traitants sont connus et les nouveaux contrats de sous-traitance sont annoncés ; il existe un droit de résiliation pour les cas de doute fondé.
- Le non-respect de la sécurité et de la protection des données (obligation de s'adapter et/ou droit de résiliation) est réglementé.
- Les obligations propres sont transmises aux sous-traitants.
- Le droit de procéder à des audits ou au moins de consulter des rapports d'audit est accordé.
- Il existe des canaux de communication et de réclamation.
- Les interlocuteurs et la procédure en cas d'incidents de sécurité existent.
- Les situations d'urgence sont préparées.
- La responsabilité civile et les amendes conventionnelles sont définies.
- La fin de contrat (en particulier lorsqu'il s'agit d'exporter, de rendre et de supprimer des données) est fixée.
- Il existe une aide pour la migration des données.
- Les valeurs de la disponibilité sont mesurées.

M-11.02 Les prestataires informatiques externes communiquent les informations suivantes au moins une fois par mois ou à tout moment sur demande :

- Degré de réalisation des valeurs de disponibilité définies (valeurs mesurées)
- Événements liés à des pannes ou à des incidents de sécurité au cours de la période considérée
- Informations concernant les modifications planifiées (p. ex. maintenance).

M-11.03 Les contrats conclus avec les prestataires cloud sont régis par la version la plus à jour du contrat-cadre de la FMH pour les services sur le cloud. Il est par ailleurs primordial que ces prestataires remplissent les « Exigences techniques et organisationnelles pour les services sur le cloud » définies par la FMH.

M-11.04 La collaboration avec les responsables de la sécurité des prestataires TIC externes est coordonnée. Cela signifie que le prestataire TIC externe,

- a accès aux présentes recommandations,
- a accès aux directives de sécurité du cabinet (voir M-1.02),
- sait, par voie de contrat, quel justificatif il doit fournir pour que la mise en œuvre des directives de sécurité (M-1.03) puisse être vérifiée, et
- met en œuvre et respecte les exigences en matière de sécurité.

Informations

I-11.01 Les contrats de prestations avec les prestataires informatiques externes repose sur les Conditions générales pour les prestations TIC, édition de janvier 2020 de la Conférence suisse sur l'informatique (CSI).

I-11.02 Le contrat-cadre de la FMH pour les services sur le cloud s'applique aux contrats de prestations avec les fournisseurs de services sur le cloud

Annexe

Déroulement et traitement

Les thèmes abordés dans ce document ont été définis avec les groupes concernés. Les personnes et les organisations suivantes ont été impliquées dans ces travaux :

- Dr Reinhold Sojer, Foederatio Medicorum Helveticorum (FMH)
- Angela Jakob, Foederatio Medicorum Helveticorum (FMH), assistante de projet
- Liliane Mollet, insecor GmbH, conseillère à la protection des données de la FMH
- Lucas Schult, Health Info Net AG (HIN), responsable informatique (CIO), 8304 Wallisellen
- Alexander Hermann, Redguard AG, 3003 Berne

Les membres suivants du corps médical se sont mis à disposition pour donner des informations concernant leur environnement informatique et ont ainsi permis de contrôler la pertinence des mesures recommandées :

- Dr méd. Steinacher Alex, Ärztezentrum Müllheim, 8555 Müllheim
- Dr méd. Koller Raphael, Herzteam Wil, 9500 Will SG
- Dr méd. Schlagenhauff Bettina, Dermacenter AG, 6403 Küssnacht am Rigi
- Dr méd. Dürrenmatt Urs, Praxis Dr. U. Dürrenmatt, 3600 Thoune
- Dr méd. Maurer Susanne, Zentrum für Adipositas- und Stoffwechselmedizin Winterthur GmbH, 8400 Winterthur
- Dr méd. Bürki Pius, Kinderzentrum Lindenpark AG, 6340 Baar

Documents utilisés et références

Pour élaborer les recommandations présentées ici, les auteurs se sont appuyés sur les documents et les bases légales du tableau ci-dessous. Ils ont également mené des interviews avec les groupes cibles afin de définir les points les plus importants et relever les enjeux et les défis actuels.

Nr.	Nom du document → Source
[1]	RS 816.111 Annexe 2 de l'ordonnance du DFI sur le dossier électronique du patient du 22 mars 2017 (état le 15 juillet 2019) → https://www.fedlex.admin.ch/eli/cc/2017/205/fr
[2]	Norme minimale pour améliorer la résilience informatique → https://www.bwl.admin.ch/bwl/fr/home/themen/ikt/ikt_minimalstandard.html
[3]	Aide à la mise en œuvre concernant la protection et la sécurité des données dans le cadre du DEP → https://www.e-health-suisse.ch/fileadmin/user_upload/Dokumente/2017/F/170627_Umsetzungshilfe_Datenschutz-Datensicherheit_f.pdf
[4]	Mehr Informationssicherheit für Klein- und Mittelbetriebe (KMU) → https://www.iktech.ch/images/10-Punkte.pdf
[5]	Mesures techniques et organisationnelles de la protection des données → https://www.edoeb.admin.ch/dam/edoeb/fr/Dokumente/aDSG/guideTOM_fr.pdf.download.pdf/guideTOM_fr.pdf

[6] La protection des données au cabinet médical selon le PFPDT
→ https://www.edoeb.admin.ch/dam/edoeb/fr/Dokumente/aDSG/leitfaden_fuer_diebearbeitungvonpersonendatenimmedizinischenbere_FR.pdf.download.pdf/leitfaden_fuer_diebearbeitungvonpersonendatenimmedizinischenbere_FR.pdf

[7] Recommandations HIN
– Mots de passe sécurisés
→ https://support.hin.ch/fr/virus-et-pourriels/des-mots-de-passe-securises
– Logiciels malveillants
→ https://support.hin.ch/fr/theme/virus-et-pourriels
– Lutter contre les spams
→ https://support.hin.ch/fr/virus-et-pourriels/guide-rapide-pour-lutter-contre-le-spam
– Cybercriminalité
→ https://www.hin.ch/fr/cybercriminalite-dangers-reels-et-mesures-efficaces

[8] Recommandations de la FMH
→ https://www.fmh.ch/fr/themes/ehealth/protection-donnees-securite/protection-des-donnees-la-loi-.cfm

Glossaire

Appareil/terminal Par appareil on entend tous les appareils qui traitent et/ou enregistrent des données de manière temporaire ou permanente, à savoir, les ordinateurs, les ordinateurs portables, les serveurs, les smartphones, les tablettes, les imprimantes et les télécopieuses.

Back-office Le back-office désigne la part d'une entreprise qui ne constitue pas le cœur opérationnel de l'entreprise mais qui sert à son maintien.

BIOS/UEFI Basic Input/Output System est un programme qui démarre lors de la mise sous tension (donc avant le système d'exploitation) et qui est nécessaire pour démarrer le système d'exploitation d'un ordinateur.

Cookies / Flash Cookie Les cookies sont des fichiers textes déposés sur le disque dur de l'appareil d'un internaute par le serveur du site visité. Les données qu'il contient sont nécessaires pour utiliser les différentes fonctions de ce site et concernent la visite du site, à savoir la durée, les données de connexion, les données saisies par l'internaute ou autre.

Cyber Security Cyber Security englobe la protection des systèmes, y c. le matériel informatique, les logiciels et les données, contre les cyberattaques.

Données des patients Les données des patients incluent toutes les informations relatives aux patients comme leur identité ou le numéro d'assurance-maladie

Données médicales Les données médicales comprennent toutes les données en lien avec la santé des patients.

Environnement informatique (TIC) TIC veut dire technologie de l'information et de la communication, simplifié par informatique. L'environnement informatique correspond à l'ensemble des ressources informatiques mises en lien.

HTTPS (Hyper Text Transfer Protocol Secure) HTTPS (protocole de transfert hypertextuel sécurisé) est une variante du protocole http offrant une couche de chiffrement comme le TLS pendant le transfert des données. L'HTTPS permet ainsi une communication chiffrée et donc une connexion sécurisée entre un serveur et un internaute éloigné.

Incident de sécurité Un incident de sécurité est un évènement qui risque de compromettre la sécurité, à savoir la confidentialité, la disponibilité ou l'intégrité des données devant être protégées.

Infrastructure de réseau L'infrastructure d'un réseau correspond à l'ensemble des applications logicielles et des composantes du matériel informatique pour relier les appareils entre eux.

Ingénierie sociale L'ingénierie sociale est une attaque utilisant des interférences personnelles aléatoires dans le but d'influencer un comportement particulier, et d'obtenir incidemment des informations confidentielles. Il s'agit notamment d'attaques d'hameçonnage et d'usurpation d'identité par courriel ou par téléphone.

IP-Adresse (adresse de protocole internet) L'adresse IP est requise pour l'envoi et la réception d'informations dans la communication sur internet.

Matériel informatique Le matériel informatique est le terme générique pour les composantes matérielles de systèmes traitant des données.

Périphériques Les périphériques sont tous les appareils en dehors de l'unité centrale, par exemple le clavier, la souris, l'écran, les lecteurs internes ou amovibles, la webcam, le pavé tactile, le haut-parleur ou le microphone.

Réseau Les réseaux relient entre eux différents appareils afin de permettre un échange de données, par exemple un réseau privé ou l'internet.

Ressources informatiques Les ressources informatiques comprennent toute la technique utilisant du matériel informatique et des logiciels dans le domaine de la communication et de l'information. Cela inclut les systèmes informatiques, comme les appareils avec ou sans accès VPN, les réseaux ou les appareils médicaux (p. ex. appareils de laboratoire, stérilisateurs, etc.), le matériel informatique comme les composantes des terminaux, des serveurs ou des réseaux, les lecteurs et les logiciels utilisés.

Sécurité des données Comme son nom l'indique, la sécurité des données traite de la sécurité de toute forme de données. Les mesures permettant de garantir la protection des données contre les abus, la falsification, la perte et les accès non autorisés aussi bien au niveau technique qu'organisationnel et personnel sont centrales.

SSL/TLS (Secure Sockets Layer/Transport Layer Security) SSL/TLS est un protocole de chiffrement pour le transfert des données sur internet. Il est notamment utilisé pour le protocole HTTPS afin de chiffrer la connexion entre un client et un serveur dans le but de préserver la confidentialité

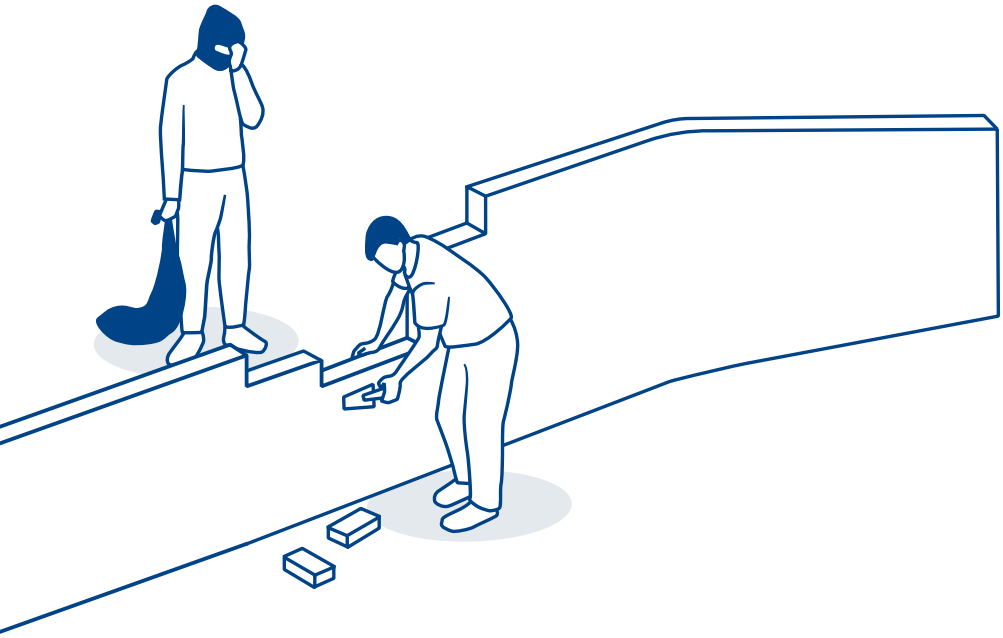
Système informatique Par système, on entend de manière général un ensemble d'éléments qui forment un tout. Dans le domaine des technologies de l'information et de la communication, le terme système inclut tout type de systèmes électroniques traitant des données, à savoir les ordinateurs, les téléphones portables, les serveurs, le cloud computing, les réseaux, les systèmes de banque de données, les systèmes d'information, les systèmes de visioconférence ou les systèmes de communication. Les appareils médicaux (p. ex. laboratoires, stérilisateurs, etc.) pouvant être raccordés à un réseau sont aussi considérés comme des systèmes informatiques.

VPN (Virtual Private Network) Le VPN (réseau virtuel privé) désigne un réseau de communication privé virtuel mis en place sans connexion matérielle, mais par un canal de communication logique et chiffré entre les partenaires de communication. Seuls les partenaires de communication appartenant à ce réseau privé peuvent communiquer et échanger des informations et des données. Les organisations utilisent le VPN pour établir une connexion de communication entre le domicile d'un membre du personnel et le réseau interne de l'organisation afin de permettre l'accès aux ressources, données et informations de l'organisation.

WiFi (Wireless Fidelity) WiFi est la désignation de la norme et de la certification des appareils capables d'établir une connexion sans fil.

WLAN (Wireless Local Area Network) Wireless Local Area Network est le nom d'une connexion sans fil via internet. Les appareils peuvent être connectés à l'internet par WLAN, c'est-à-dire dans fil.

Impressum
Edition : FMH – Fédération des médecins suisses, Berne
Texte : Redguard AG, Berne
Infographie/illustration : Hahn+Zimmermann, Berne
Publication : décembre 2019 (version mars 2023)
www.fmh.ch




Notice
1
2
3


Notice


HR
BPM
100
60
80