FMH

D2

Sécurité informatique des cabinets médicaux

Onze recommandations

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

Madame,
Monsieur,

La transformation numérique et les interconnexions accrues dans le domaine de la santé ouvrent de nouvelles perspectives et contribuent à l'amélioration des processus de traitement et au développement de la qualité en médecine.

Au-delà de ces avantages, elles comportent également des risques dans le domaine de la sécurité et de la protection des données : les cyberattaques contre les données de santé et les infrastructures informatiques (TIC) peuvent porter atteinte à la vie privée des patients, restreindre considérablement les activités quotidiennes d'un cabinet médical, causer un préjudice financier et nuire à la réputation ou influencer le traitement des patients.

Chaque cabinet médical est chargé de garantir la protection et la sécurité des données qu'il traite. Dans la loi sur la protection des données, le législateur qualifie les données médicales de données personnelles sensibles ce qui exige la mise sur pied d'un nombre important de mesures pour une protection adéquate de ces données.

La mise en place, l'entretien et la maintenance d'une infrastructure informatique sécurisée 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 présentes recommandations sont là pour vous accompagner face à ces nouveaux défis et vous aider à mettre en place, maintenir et optimiser la sécurité et la protection des données dans votre cabinet.

Dre Yvonne Gilli

Présidente de la FMH

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.

Sommaire

Aperçu 4

Recommandation 1 : définir les responsabilités et fixer les directives informatiques (TIC) 5

Recommandation 2 : dresser l'inventaire des ressources informatiques 6

Recommandation 3 : restreindre les droits d'accès et gérer les utilisateurs 7

Recommandation 4 : sensibiliser les collaborateurs à la protection des données 8

Recommandation 5 : protéger les appareils contre les logiciels malveillants 9

Recommandation 6 : protéger le réseau 10

Recommandation 7 : configurer et entretenir l'infrastructure informatique 11

Recommandation 8 : assurer des sauvegardes fiables 12

Recommandation 9 : assurer la sécurité des données échangées 13

Recommandation 10 : définir une procédure de gestion des incidents de sécurité 14

Recommandation 11 : mandater des prestataires externes et superviser leur travail 15

Aperçu

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 cabinets et s'appliquent aux cabinets jusqu'à une douzaine de médecins environ. Elles s'adressent en premier lieu aux médecins, à leurs collaborateurs et aux tiers qu'ils auront mandatés (prestataires TIC, p. ex.).

Objectif

Les recommandations de la FMH visent une protection adéquate des données personnelles sensibles gérées par les cabinets médicaux. Elles répondent notamment aux exigences légales en la matière.

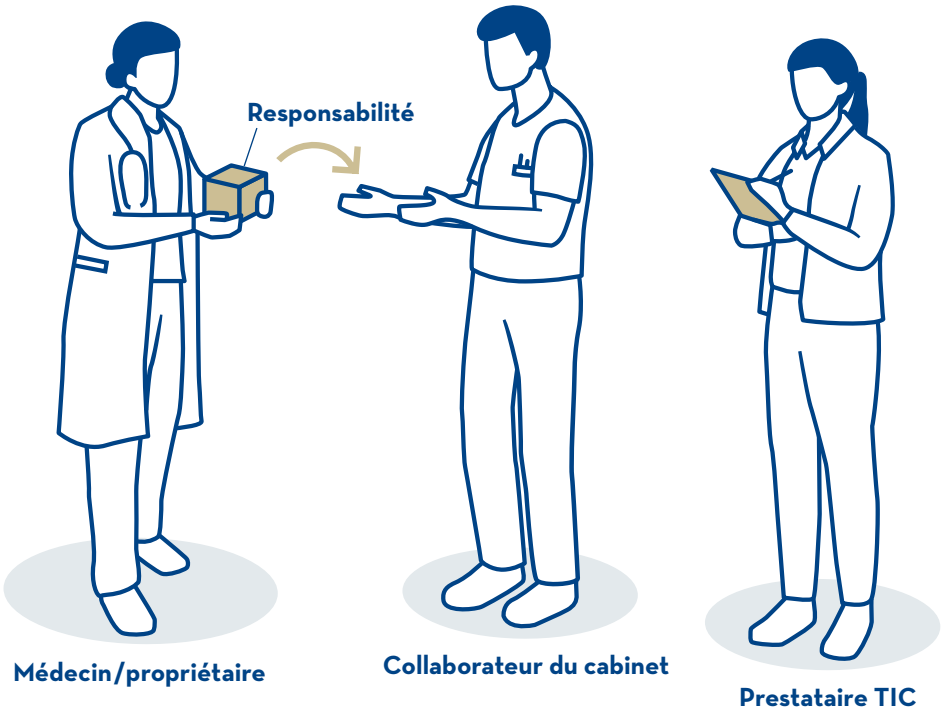
Structure

Le présent document donne une vue d'ensemble des recommandations de la FMH pour une protection informatique élémentaire des cabinets médicaux. Les recommandations et les mesures présentées ici sont décrites plus en détail dans le document « D3 Exigences minimales pour la sécurité informatique des cabinets médicaux ».

	Représentation graphique	Programme en 11 points	Mesures détaillées
Médecin/propriétaire	○	●	○
Collaborateur du cabinet	○	●	○
Prestataire TIC	×	×	○

R1

Définir les responsabilités et fixer les directives informatiques (TIC)

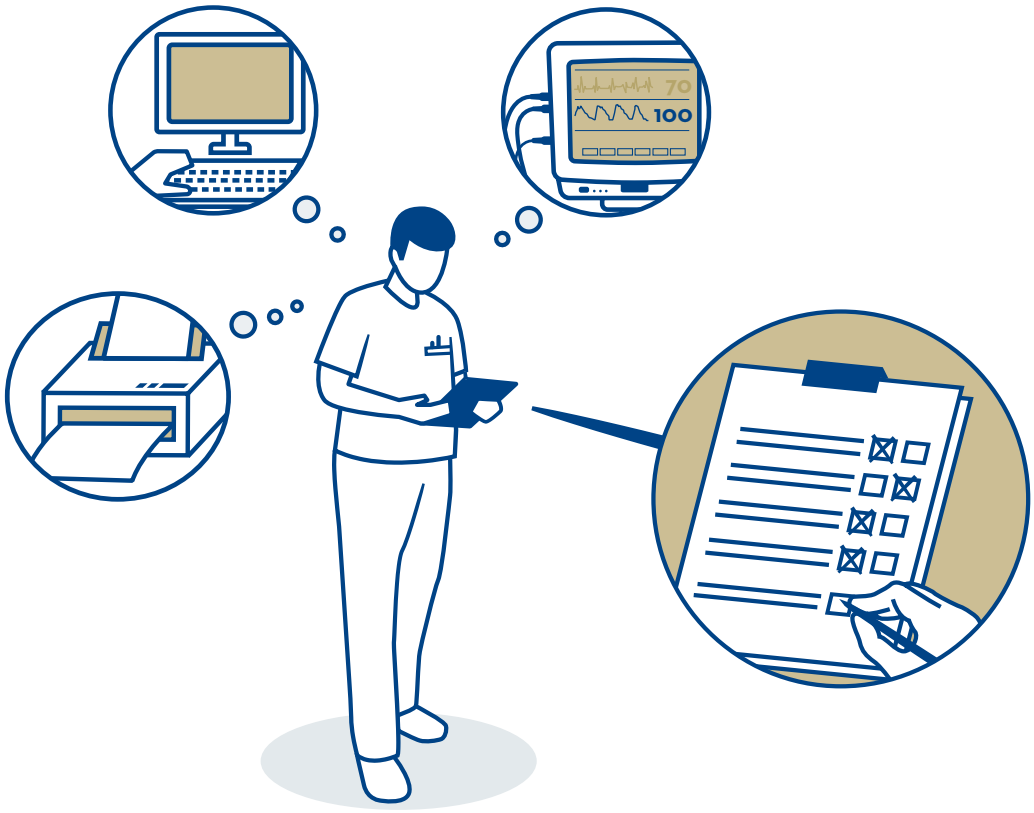


Définir les responsabilités, les tâches et les compétences permet de donner aux questions de sécurité informatique et de protection des données la place qui leur revient dans la gestion d'un cabinet. Tout propriétaire de cabinet est responsable de la protection et de la sécurité des données (responsable PSD). À ce titre, il en a la responsabilité opérationnelle et se charge de la mise en œuvre des mesures nécessaires. Il peut assumer ce rôle lui-même, ou le confier soit à un prestataire informatique externe, soit à un collaborateur du cabinet.

Le cahier des charges d'un responsable PSD comprend la définition de directives de sécurité et la mise en œuvre des mesures ad hoc. Les directives de sécurité portent sur la gestion et l'échange de données, l'utilisation des outils informatiques, ainsi que la protection des terminaux et du réseau. La mise en œuvre des directives peut s'opérer au niveau technique, organisationnel ou personnel, ou à plusieurs niveaux à la fois.

Le rôle du responsable PSD est à distinguer de celui du responsable informatique, qui dirige la mise en place, l'exploitation et l'entretien de l'infrastructure. Le responsable PSD définit les exigences en matière de sécurité et de protection des données. Il délègue leur implémentation au responsable informatique et surveille leur mise en œuvre.

R2 Dresser l’inventaire des ressources informatiques



Une protection efficace des données exige que l’on dispose d’équipements fiables. De manière générale, on ne peut protéger que ce dont on connait l’existence.

C’est pourquoi on s’efforcera, à l’aide d’attributs prédéfinis, de répertorier l’ensemble des ressources informatiques dans une liste d’inventaire et de les classer selon le caractère sensible des données et des informations qu’elles vont permettre de gérer. Cette liste peut être incorporée au registre des activités de traitement.

Elle aide à la planification et à la mise en œuvre des mesures de sécurité et permet de réagir plus vite et plus efficacement en cas d’incident. On la mettra à jour régulièrement.

Lors de la mise hors service d’installations, et en particulier d’ordinateurs, toutes les données seront effacées complètement et de façon irréversible.

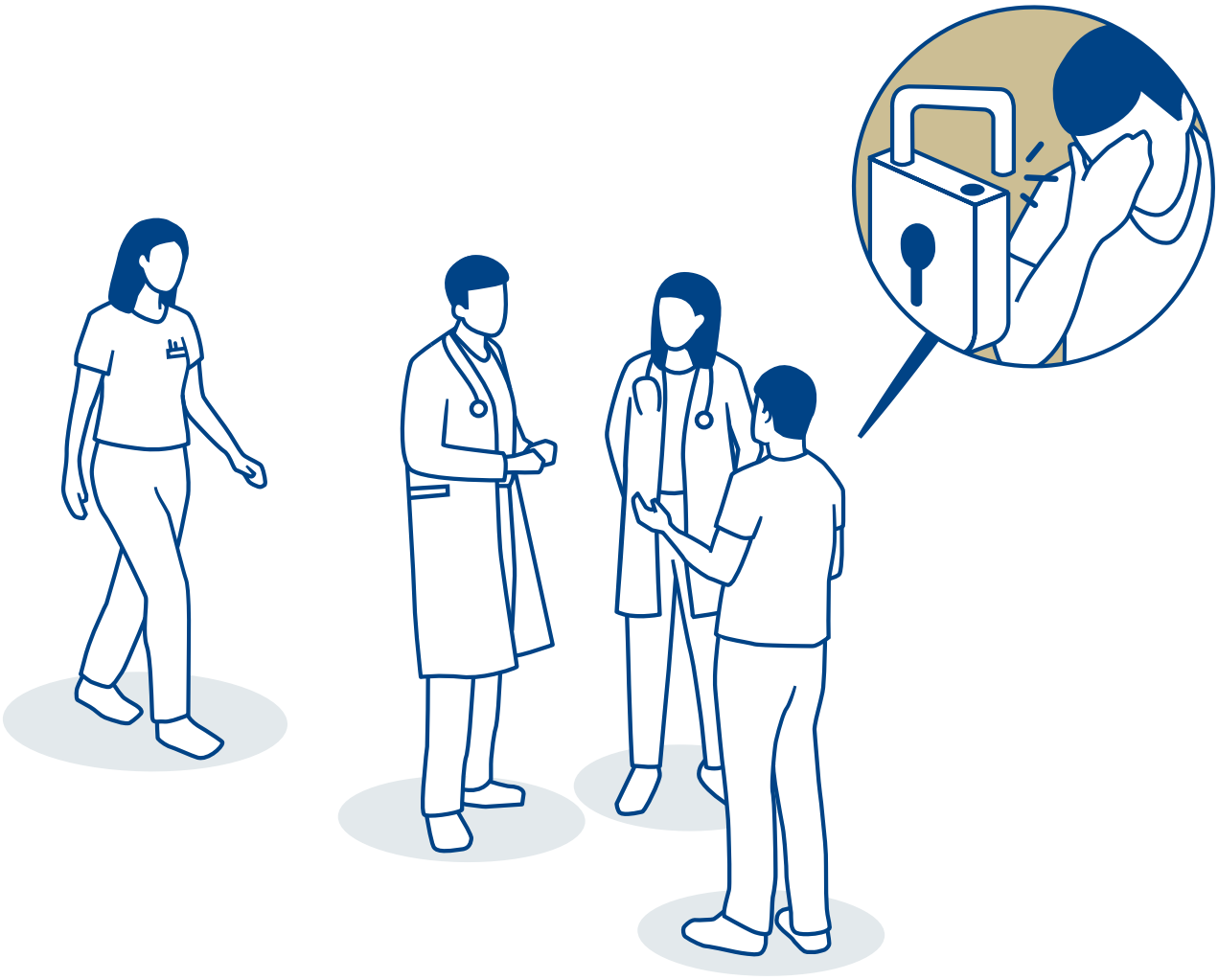
R3 Restreindre les droits d'accès et gérer les utilisateurs

Restreindre les droits d'accès permet de réduire les risques d'abus. Les utilisateurs et les administrateurs devraient bénéficier uniquement des droits d'accès indispensables à l'accomplissement de leurs tâches quotidiennes (principe Need to know). Les mots de passe doivent compter au moins dix caractères et remplir divers critères de sécurité supplémentaires. Ils doivent tous 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.

Pour accéder aux données médicales des patients, chaque collaborateur du cabinet doit disposer d'un compte utilisateur propre. Pour accéder à internet, les collaborateurs utiliseront des comptes utilisateurs personnels distincts. Le système du cabinet ne doit être accessible qu'après identification à deux facteurs.

Toute activité sur un compte utilisateur, p. ex. les tentatives de connexion et déconnexion, est enregistrée et surveillée, afin de détecter les comportements inappropriés et assurer la traçabilité des opérations.

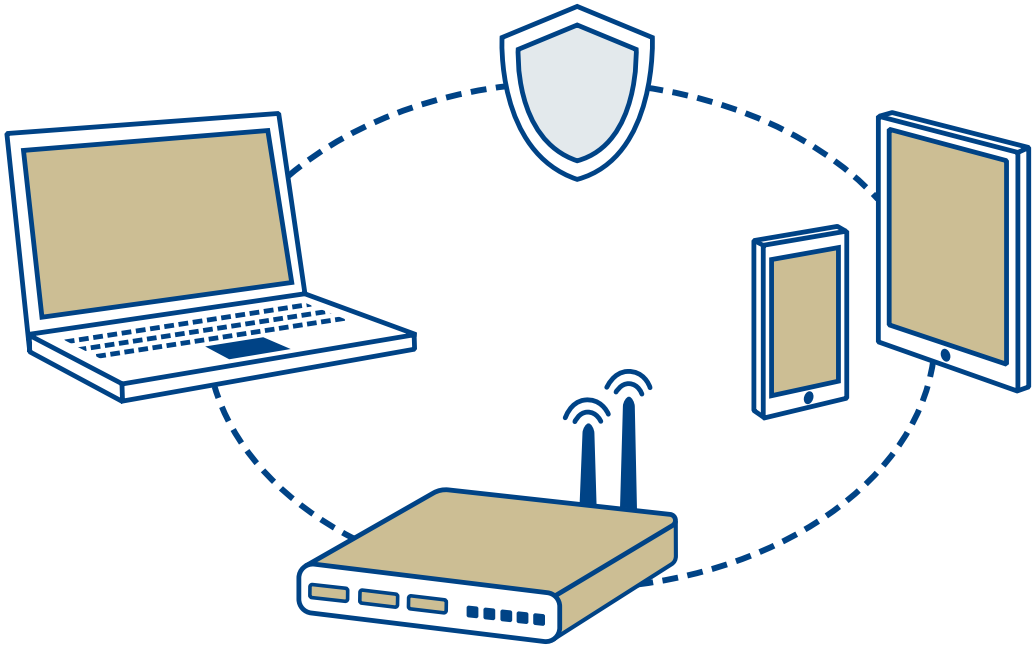
R4 Sensibiliser les collaborateurs à la protection des données



Le personnel d'une entreprise constitue une cible privilégiée des pirates informatiques qui tentent fréquemment d'accéder aux infrastructures TIC et aux données par des attaques d'ingénierie sociale. C'est dire si la sensibilisation des collaborateurs à ces questions est l'un des piliers de toute stratégie visant à assurer la protection et la sécurité des données.

Il est possible de rendre les collaborateurs attentifs aux risques de piratage informatique et à la nécessité de manier les données sensibles avec précaution. Pour cela, il existe plusieurs canaux, comme des cursus de formation, des brochures, ou encore une information ciblée du personnel lors d'incidents de sécurité. Parmi les autres moyens d'encourager un comportement responsable, on peut citer la définition de consignes relatives aux mots de passe et codes PIN, et au maniement correct des outils informatiques et des données, ainsi que de marches à suivre en cas d'incident. On veillera à informer les collaborateurs aussi bien lors de leur entrée en fonction que par la suite (mais aussi au moment de leur départ), et à intervalles réguliers, de façon à maintenir durablement un haut niveau d'attention aux impératifs de protection et de sécurité des données ainsi que de gestion avisée des données.

R5 Protéger les appareils contre les logiciels malveillants

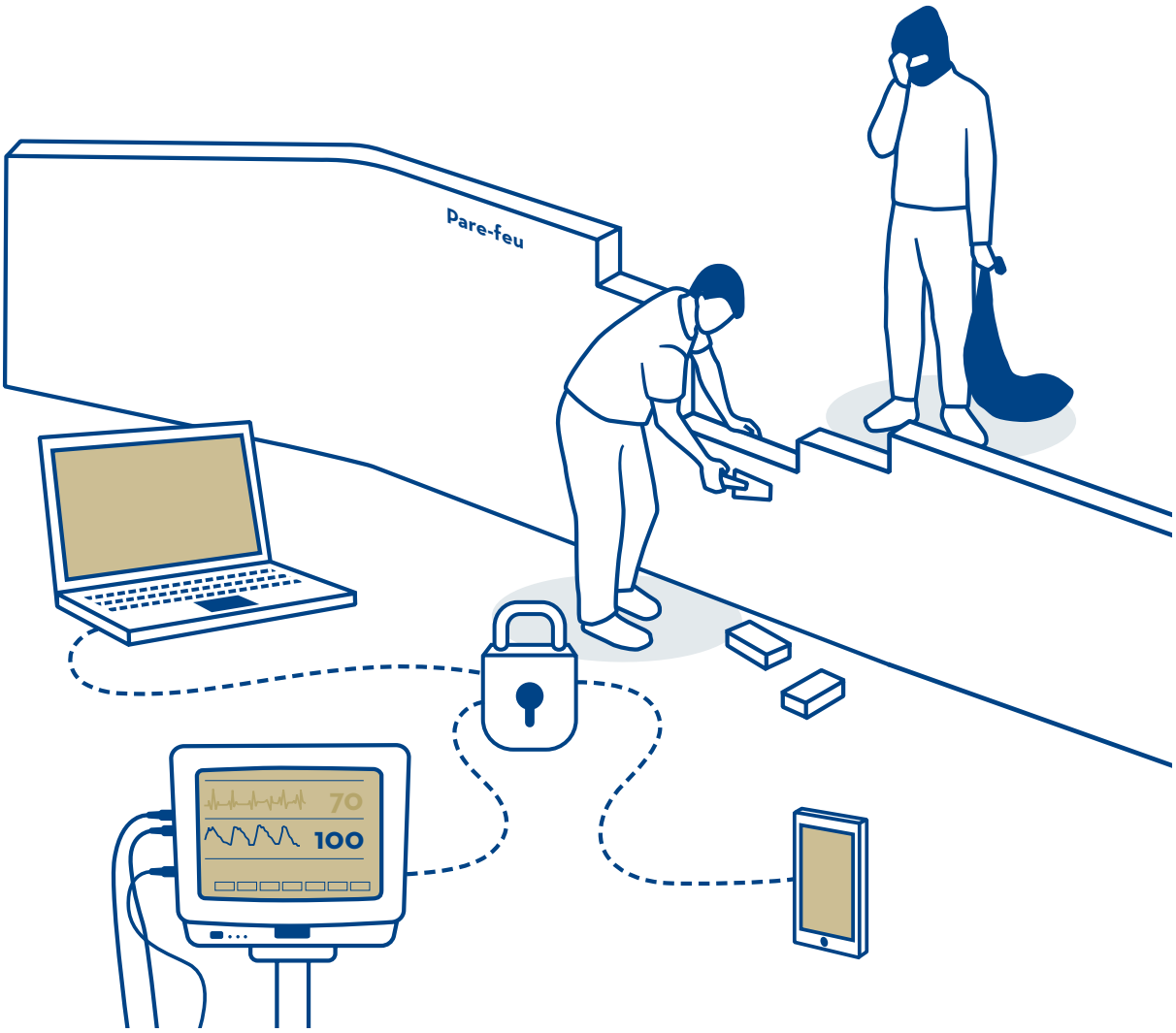


Les terminaux informatiques (téléphones et ordinateurs portables) peuvent être facilement contaminés par des logiciels malveillants, d'où la nécessité d'équiper chacun d'eux d'un antivirus à jour. Configuré de manière à vérifier systématiquement les fichiers chaque fois que quelqu'un y accède, un antivirus permet de déceler la présence éventuelle d'éléments nuisibles. De plus, il convient d'actualiser les signatures antivirus au moins une fois par jour. Enfin, on n'oubliera pas de mettre régulièrement à jour le système d'exploitation.

Les terminaux utilisés dans les cabinets ne devraient pas être utilisés à des fins privées.

Ces quelques précautions suffisent à limiter considérablement les risques de contamination. Il faut toutefois garder à l'esprit que les antivirus ne reconnaissent que les logiciels malveillants qu'ils connaissent. Il n'est donc jamais possible d'assurer une protection intégrale, et il est capital de sensibiliser aux risques potentiels, notamment lors de l'envoi et de la réception de courriels et de pièces jointes.

R6 Protéger le réseau

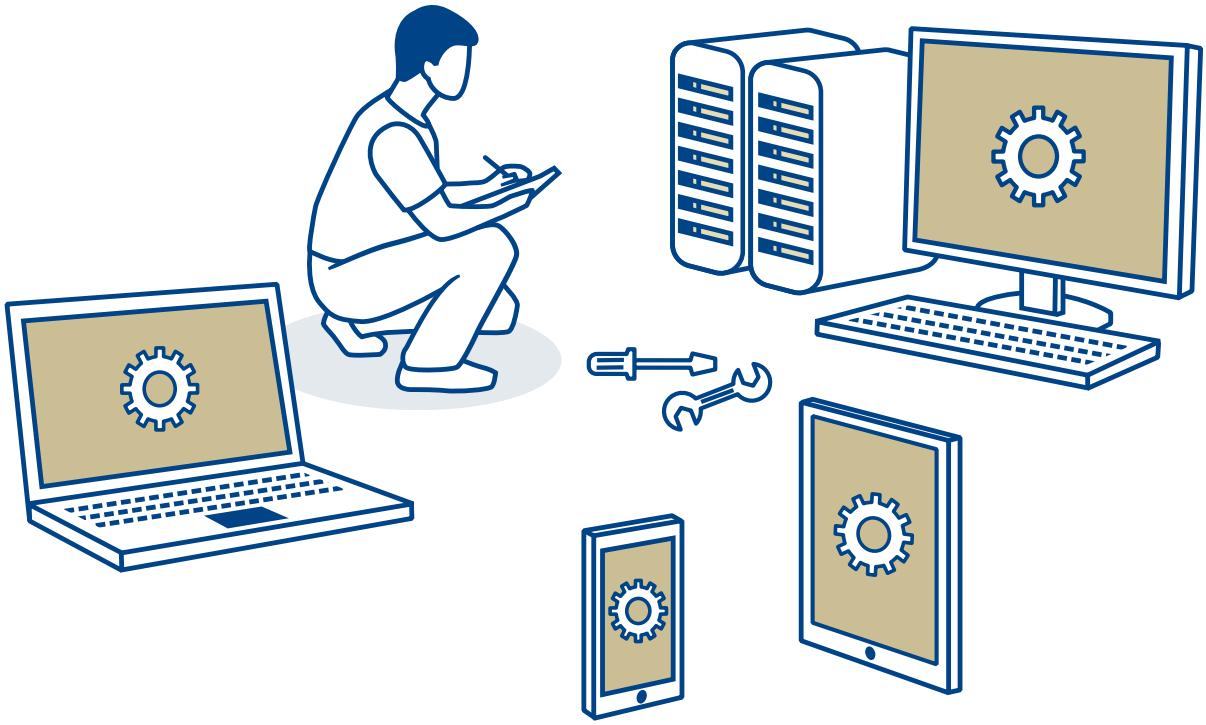


Il est essentiel de protéger le réseau informatique d'un cabinet médical contre tout accès non autorisé pour empêcher que des tiers puissent écouter des conversations ou voler des données.

Pour éviter tout accès non autorisé au réseau interne d'un cabinet, on veillera à mettre en place des mesures de sécurité aux points d'accès à internet et aux points de raccordement avec ou sans fil vers le réseau local.

Pour protéger les points de raccordement entre le réseau informatique d'un cabinet et internet, on veillera à installer et configurer des dispositifs pare-feu. Ces derniers servent à réguler le trafic de données et remplissent diverses fonctions de sécurité, comme une analyse antivirus du réseau. Les boîtiers de raccordement non utilisés doivent être verrouillés, car ils offrent une porte d'entrée aux tiers non autorisés. Les connexions sans fil, particulièrement le WiFi, seront protégés par mot de passe.

R7 Configurer et entretenir l'infrastructure informatique

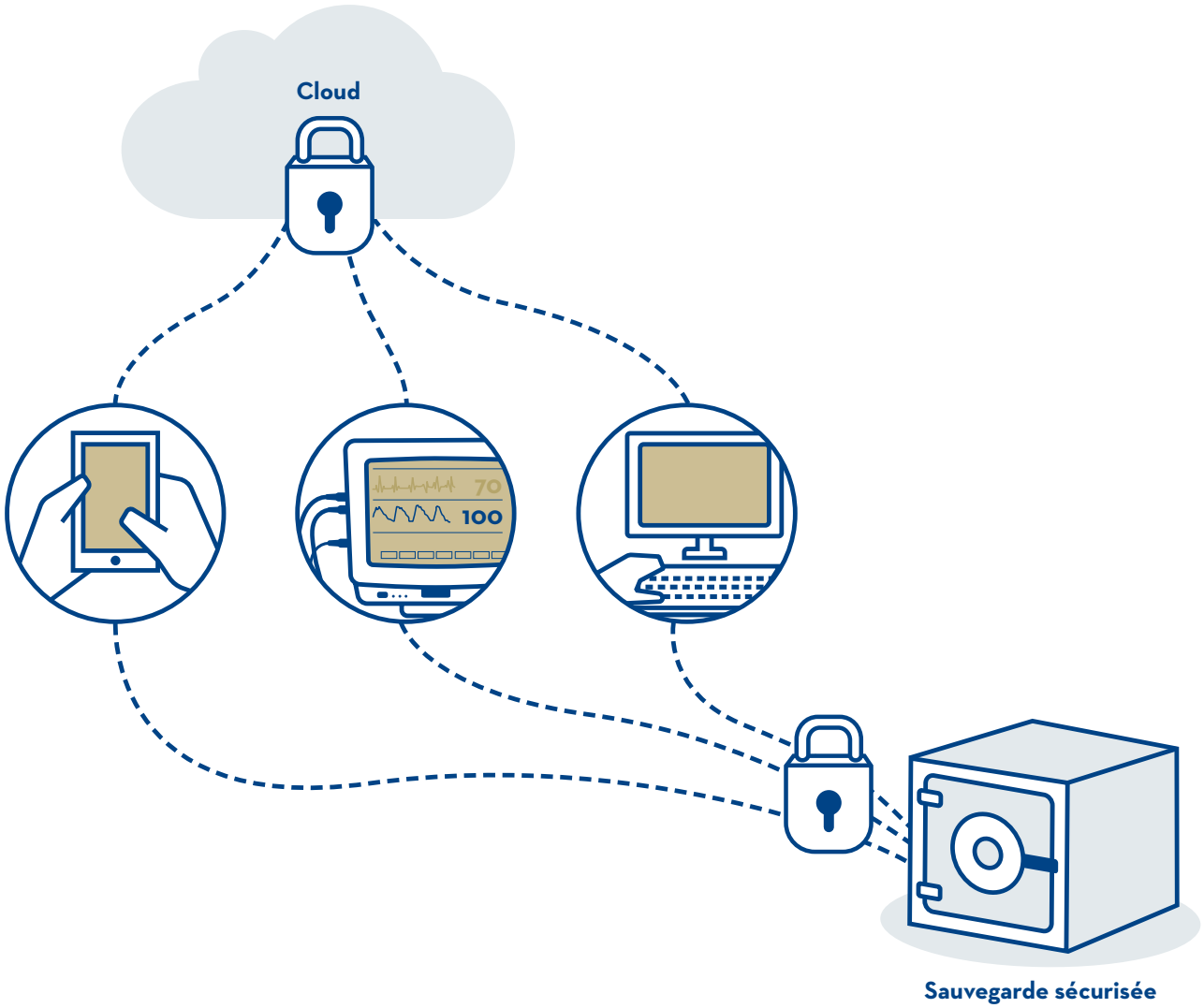


Une bonne configuration des systèmes et des éléments de réseau permet de réduire l'exposition, et donc la probabilité et les conséquences d'une cyberattaque.

Il est difficile, voire impossible d'intervenir sur des systèmes TIC tels que les appareils de laboratoire lorsqu'ils sont intégralement livrés par des tiers, du fait d'obstacles d'ordre contractuel ou technique. On gérera ce type d'équipements à part, en les déplaçant par exemple dans une zone de réseau réservée, étant donné que pour la plupart, il est impossible de les mettre à jour ou de les doter de configurations de sécurité.

On prendra de préférence plusieurs précautions à la fois pour protéger les systèmes TIC, comme la mise à jour automatique des systèmes de sécurité, le chiffrement des disques durs ou l'utilisation de mots de passe robustes pour les comptes utilisateurs. À des fins de contrôle opérationnel, les systèmes et applications TIC devraient enregistrer et évaluer en continu l'activité des utilisateurs, et donner l'alerte en cas de panne d'un des systèmes.

R8 Assurer des sauvegardes fiables

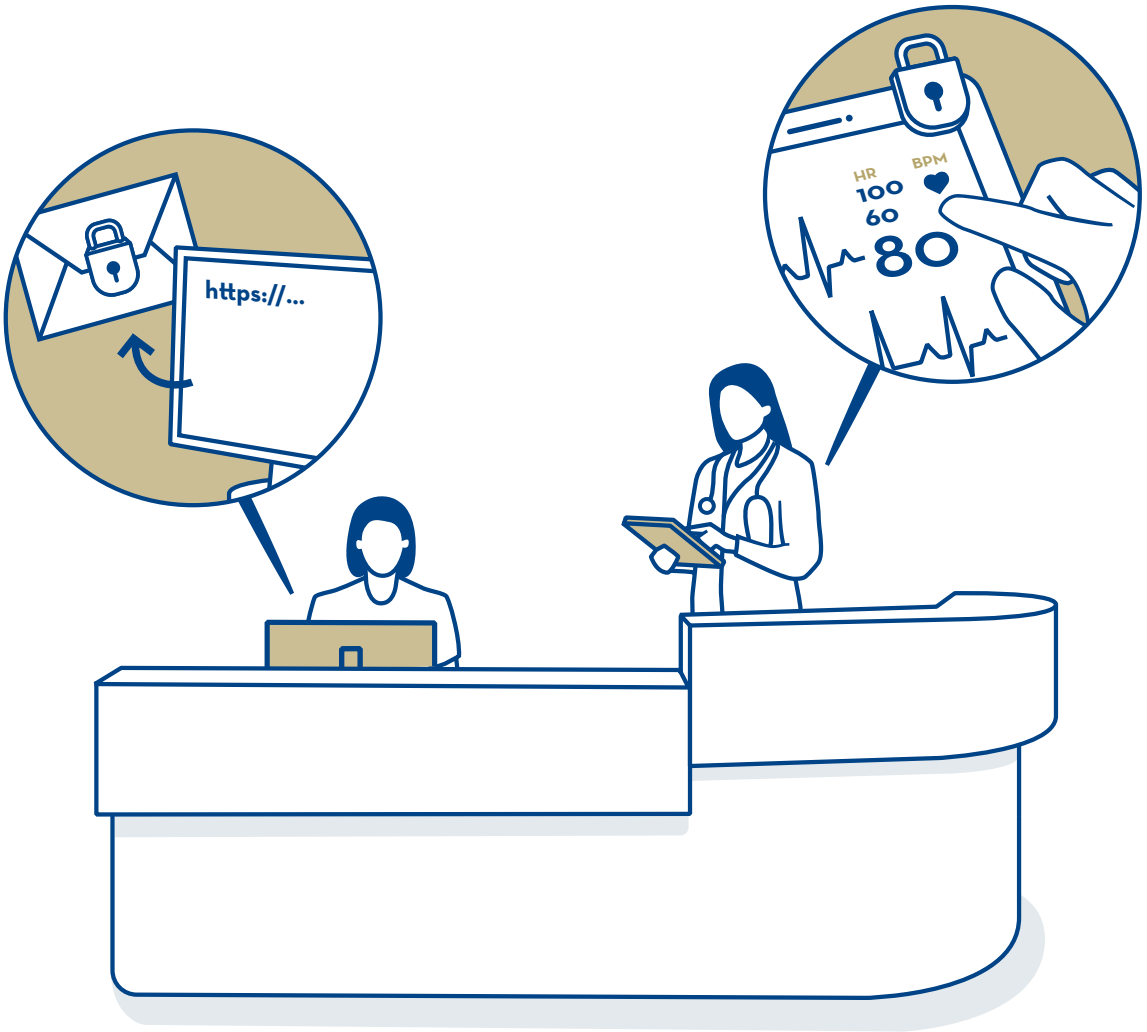


Il est important d'assurer la sauvegarde régulière (backup) de la totalité des données pour se prémunir des risques de pertes liés à une mauvaise manipulation par un collaborateur, à une panne de matériel ou à l'action d'un logiciel malveillant. Pour assurer la confidentialité et l'intégrité des données sauvegardées, on veillera aussi à définir et enregistrer les droits d'accès et d'utilisation des données initiales pour le cabinet.

La sauvegarde sera effectuée à intervalles réguliers et les données stockées en dehors des locaux du cabinet médical. On testera par ailleurs au moins une fois par an la possibilité de restaurer les données à partir des sauvegardes.

La sauvegarde sur le cloud doit également respecter les dispositions de la loi sur la protection des données et le secret professionnel, ce qui exige des mesures techniques supplémentaires.

R9 Assurer la sécurité des données échangées



Il est préférable de chiffrer les données personnelles sensibles pour s'assurer qu'elles ne tombent pas entre les mains de tiers non autorisés. Cela permet de garantir que seules les personnes qui en sont autorisées puissent les consulter, les supprimer ou les modifier et d'éviter que les données soient modifiées sans que personne ne s'en rende compte.

Les données de patients échangées par e-mail seront systématiquement chiffrées. L'envoi de données par fax ne permet pas le chiffrement et devrait à ce titre être maintenu au strict minimum. L'accès à des applications sur internet ne doit être possible que par un canal protégé, p. ex. le protocole HTTPS. On n'enverra jamais de données médicales ou d'identifiants tels que des mots de passe sur un canal non chiffré.

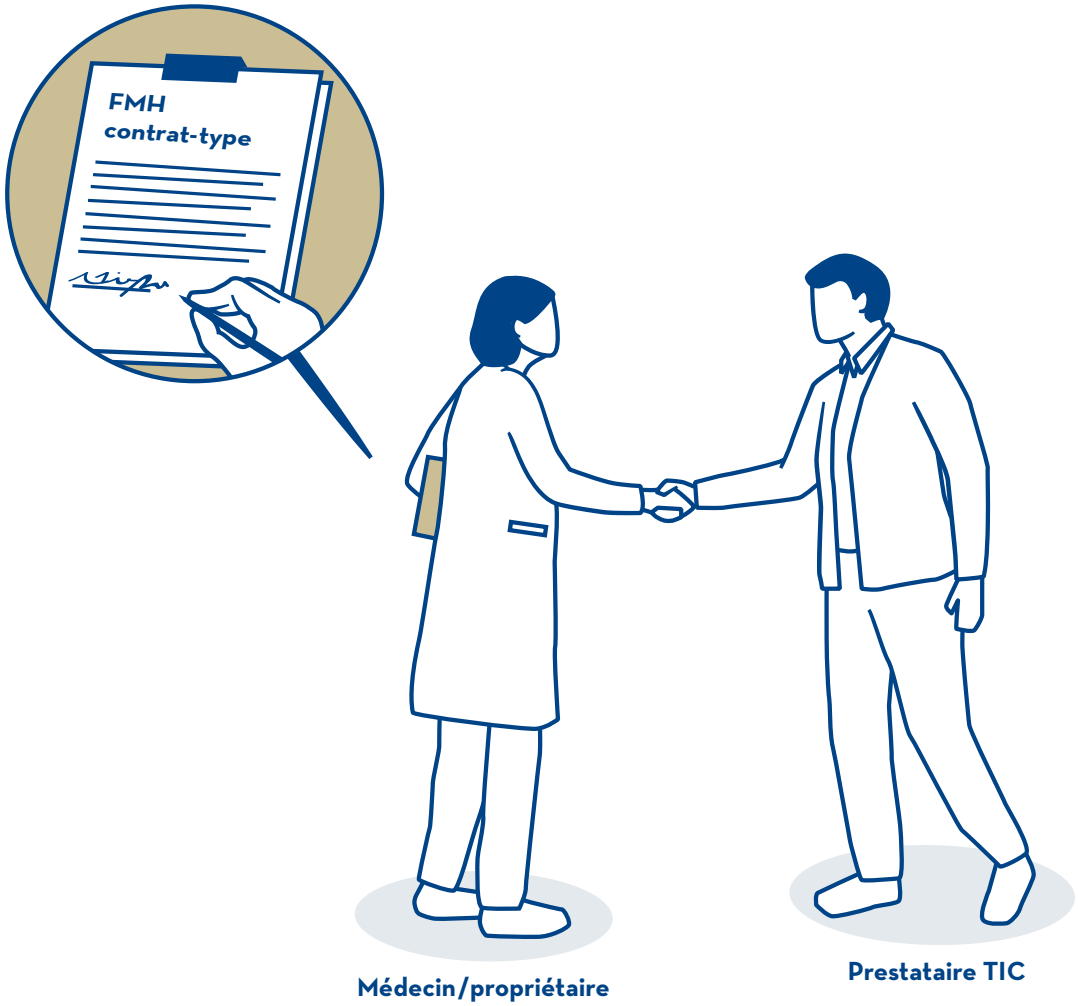
R10 Définir une procédure de gestion des incidents de sécurité

Les incidents de sécurité sont des événements qui compromettent la confidentialité, l'intégrité et la disponibilité des informations et des données. Le phishing (hameçonnage), l'exploitation de failles de sécurité ou les attaques de logiciels malveillants (virus, vers informatiques ou chevaux de Troie) sont des exemples d'incidents pouvant avoir un impact énorme sur le fonctionnement d'un cabinet médical. Il est important de prendre des précautions d'ordre technique ou organisationnel pour être en mesure de détecter et de traiter de manière rapide et efficace ces incidents.

On définira par exemple un interlocuteur auquel le personnel du cabinet devra s'adresser en cas d'incident. La centrale d'alerte et ces coordonnées devront être connues de l'ensemble du personnel. On veillera par ailleurs à élaborer et à diffuser au personnel des notices contenant un descriptif détaillé de la procédure à suivre ainsi que des analyses de cas pratiques.

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.

R11 Mandater des prestataires externes et superviser leur travail



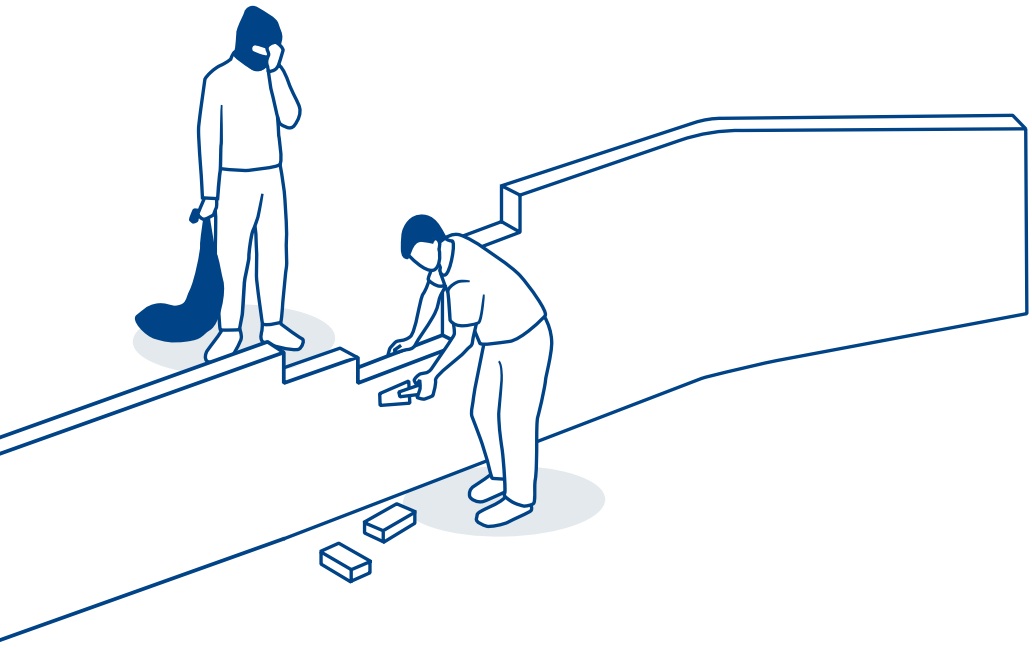
Il est possible de mandater un prestataire externe pour assurer l'installation, l'exploitation, ou encore l'entretien et la maintenance des infrastructures informatiques. Le choix du prestataire s'appuiera sur une évaluation approfondie du service proposé, et l'on veillera à superviser son travail par le biais de rapports mensuels ou autres, en fonction des besoins.

Pour coordonner la collaboration avec les responsables sécurité d'un prestataire TIC externe, on veillera à mettre à leur disposition les présentes recommandations, les directives de sécurité internes, et à définir contractuellement les justificatifs attestant le respect des directives de sécurité. Tout prestataire TIC externe devrait définir par écrit comment il entend respecter et mettre en œuvre les directives de sécurité.

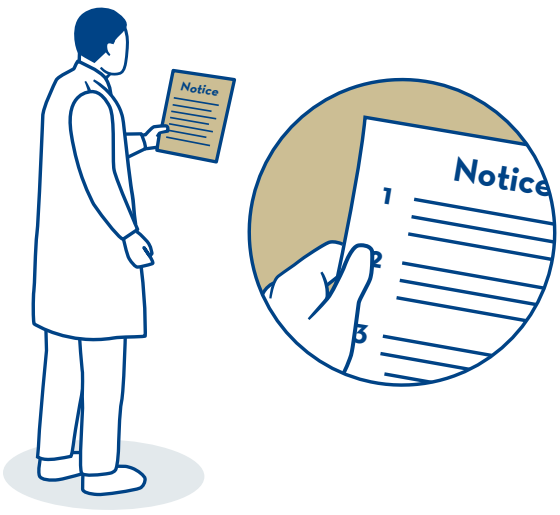
Concernant les conventions de prestations avec un prestataire informatique externe, il est possible d'appliquer les conditions générales pour les prestations TIC, édition de janvier 2020, pouvant être consultées sur le site internet de l'Administration numérique suisse (ANS). Pour les contrats de prestations avec les prestataires de services sur le cloud, la FMH recommande son contrat-cadre pour les services sur le cloud.

Glossaire
Le glossaire peut être consulté en ligne en suivant ce lien :
https://www.fmh.ch/fr/themes/ehealth/informatique-cabinet-medical.cfm

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



FMH
contrat-type


Notice
Notice
1
2
3