Ne pas négliger la sécurité informatique au cabinet

Reinhold Sojer

Dr rer. biol. hum., chef de la division Numérisation/eHealth, FMH

Le système suisse de santé, c'est aussi près d'un million et demi de gigaoctets de données traitées chaque année et plus de 300 millions de feuilles de papier contenant des données médicales de patients. Au total, 76 000 gigaoctets sont générés par les seuls cabinets de médecins de famille, qui utilisent de plus en plus un système informatique pour les dossiers de leurs patients [1]. A l'instar des dossiers physiques et matériels, les données électroniques doivent être protégées contre tout accès non autorisé, notamment à la lumière de l'utilisation accrue des réseaux informatiques. Les cyberattaques contre les données de santé et les infrastructures peuvent restreindre considérablement les activités quotidiennes d'un cabinet médical, causer un préjudice financier, nuire à la réputation du cabinet ou compromettre la sécurité des patients. Le législateur qualifie de données personnelles sensibles les données qui transitent dans un cabinet médical et qui, de ce fait, doivent être protégées par des mesures techniques et organisationnelles adéquates. Ces mesures visent à réduire le risque d'attaques informatiques exploitant les failles de sécurité et compromettant la confidentialité, l'intégrité et la disponibilité des données des patients. La confidentialité est compromise lorsque, par exemple, les données des patients sont échangées sans être chiffrées, tandis que la disponibilité des données risque d'être interrompue par une défaillance du système. Par contre, un défaut de disponibilité des systèmes n'est pas forcément le résultat d'une attaque ciblée, comme celle du cheval de Troie WannaCry en 2017, qui a contaminé plus de 230 000 ordinateurs dans 150 pays différents. Début 2018, une «simple» erreur logicielle chez Swisscom s'était conclue par plus de 5000 cabinets médicaux coupés du réseau téléphonique pendant plusieurs heures [2].

La Confédération a publié pour la première fois en 2018 des standards minimaux afin de protéger les infrastructures à risque, comme celles des fournisseurs d'énergie et d'eau, ou les hôpitaux. En revanche, aucun standard n'existe pour les petites et moyennes entreprises et notamment pour les cabinets médicaux. En cas d'incident, le médecin porte l'entière responsabilité de la sécurité et de la protection des données, et du fonctionnement de l'infrastructure informatique de son cabinet. Compte tenu des ressources disponibles dans chaque cabinet, cette tâche représente un véritable défi pour leurs propriétaires.

Dans ce contexte, la FMH a élaboré des exigences minimales pour la sécurité informatique des cabinets médicaux. Destinées à ses membres, ces exigences permettent d'atteindre un niveau de protection adéquat et de répondre aux dispositions de la loi sur la protection des données. Elles se présentent sous forme de recommandations se déclinant en plusieurs mesures sur les droits d'accès, l'administration des utilisateurs, la protection du réseau ou la sensibilisation du personnel. La mise en œuvre et le respect de ces mesures ne peuvent cependant pas offrir une protection totale en cas de cyberattaque. En revanche, le propriétaire d'un cabinet et son équipe pourront mieux surmonter un *éventuel* incident de sécurité, qui se produirait malgré toutes les mesures de protection, s'ils y sont préparés.

Crédit photo
Hahn + Zimmermann

Références

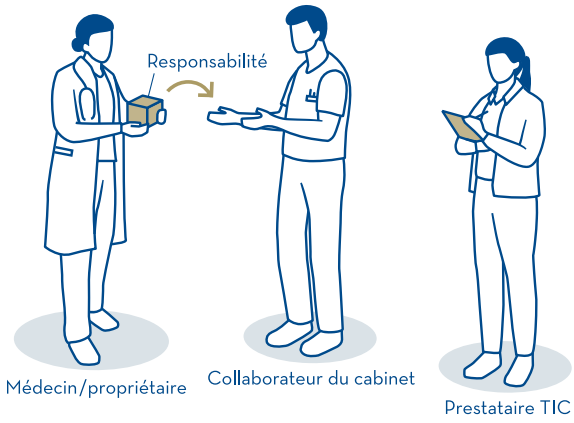
1 Swisscom Health: les données médicales suisses aujourd'hui et demain, 2017.
2 La FMH a élaboré des recommandations à ce sujet: https://www.fmh.ch/fr/themes/ehealth/informatique-cabinet-medical.cfm#i135221

Les recommandations peuvent être consultées à l'adresse suivante: https://www.fmh.ch/fr/themes/ehealth/informatique-cabinet-medical.cfm

Dr Reinhold Sojer
Chef de la division Numérisation/eHealth, FMH
Elfenstrasse 18
Case postale 300
CH-3000 Berne 15
Tél. 031 359 12 04
reinhold.sojer[at]fmh.ch

Exigences minimales pour la sécurité informatique des cabinets médicaux

Onze recommandations



R1

Définir les responsabilités et fixer les directives informatiques (TIC)

R2

Dresser l'inventaire des ressources informatiques

R3

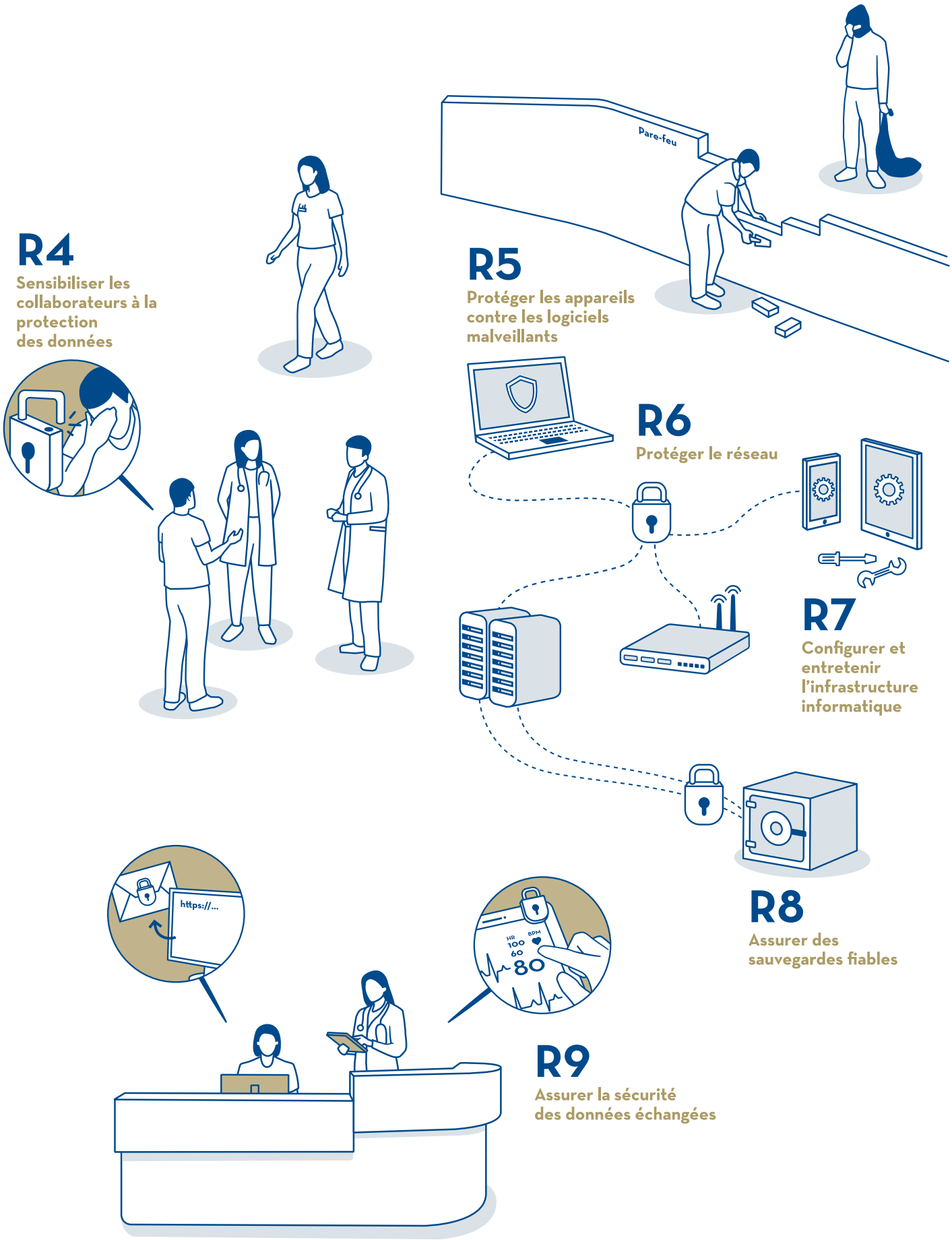
Restreindre les droits d'accès et gérer les utilisateurs

R11

Mandater des prestataires externes et superviser leur travail

R10

Définir une procédure de gestion des incidents de sécurité



R4
Sensibiliser les collaborateurs à la protection des données

R5
Protéger les appareils contre les logiciels malveillants

R6
Protéger le réseau

R7
Configurer et entretenir l'infrastructure informatique

R8
Assurer des sauvegardes fiables

R9
Assurer la sécurité des données échangées