hôpital fribourgeois
freiburger spital

Règlement HFR sur l'utilisation des moyens informatiques

1 Objectif

Le présent règlement a pour objectif de contribuer à la préservation de la sécurité du système d'information (SI) de l'HFR. Il fixe les règles d'utilisation des moyens informatiques et de télécommunication mis à disposition de ses collaborateurs (ci-après les utilisateurs) par l'HFR. Il explicite et complète la législation en vigueur en matière de protection des données.

Le règlement a pour objet de définir les droits, devoirs et responsabilités des utilisateurs du SI HFR.

2 Périmètre

Le règlement s'applique à tous les utilisateurs internes et externes de l'HFR disposant d'un accès au SI HFR, définissant leurs droits, devoirs et responsabilités. Il vise l'utilisation de toutes les ressources informatiques telles qu'ordinateurs (pc), laptops, imprimantes, serveurs, applications, partages de fichiers, VPN, messagerie électronique, téléphonie IP, internet, smartphones ainsi que toutes les données traitées dans le SI. L'utilisation du matériel privé expressément autorisé par la direction des systèmes d'information et opérations (DSIO) fait également partie du périmètre du présent règlement.

3 Règles d'utilisation

3.1 Internet (y compris réseaux sociaux et cloud)

Les principes d'utilisation du réseau internet (y c. réseaux sociaux et cloud) sont définis par l'Ordonnance (122.70.17) relative à la surveillance de l'utilisation d'Internet par le personnel de l'Etat. Il en ressort le principe de base (cf. art. 4 al. 1) que :

L'utilisation d'Internet est réservée à des fins professionnelles.

Toutefois, l'utilisation occasionnelle d'Internet à des fins privées, y compris celle du courrier électronique et des médias sociaux, est tolérée dans les limites résultant de l'obligation de service de consacrer tout son temps à son travail (cf. art. 4 al. 2 renvoyant à l'art. 58 al. 1 LPers).

L'utilisation à des fins privées doit aussi remplir les conditions suivantes :

- ne pas entraver la bonne marche du service ;
- ne pas perturber le réseau ;
- ne pas relever d'une activité lucrative ;
- ne pas être illicite.

Internet étant un réseau ouvert et donc n'offrant aucune garantie en termes de sécurité, les règles suivantes doivent être respectées :

- Aucune donnée sensible (p. ex : données médicales) de l'HFR ne peut être transmise, stockée ni traitée sur Internet (p. ex : transmission à un tiers, recours à des services cloud, etc.) sans l'accord d'une instance autorisée de l'HFR ni sans les mesures de protection nécessaires (chiffrement des données, etc.).

  Des exceptions ne sont tolérées qu'en cas d'impérative nécessité : lorsqu'il s'agit de disposer d'un avis médical urgent à distance, l'utilisation d'une application cloud est tolérée dans des cas extrêmes, sous condition que le patient ne soit pas identifiable,

qu'il y ait un contact téléphonique préalable et que l'image ou la vidéo transmise soit supprimée immédiatement après réception (par l'expéditeur et le destinataire).

- Il est interdit de stocker des documents professionnels sur un cloud public (p. ex : DropBox, GoogleDrive, etc.) ou sur un cloud privé (p. ex : NAS privé) sans l'accord d'une instance autorisée de l'HFR ni sans les mesures de protection nécessaires (chiffrement des données, etc.).
- L'utilisation des réseaux sociaux ou le déploiement d'autres activités sur Internet ne doivent en aucun cas nuire à la réputation de l'HFR ni à celle de ses partenaires.
- La publication de tout contenu multimédia relatif à l'HFR ou mettant en scène des collaborateurs est strictement interdite sans l'accord du service de communication.

3.2 Messagerie électronique

L'utilisation de la messagerie électronique est soumise aux règles suivantes :

- L'échange d'informations professionnelles ne doit intervenir que par boîtes mails professionnelles. Il est en outre strictement interdit d'envoyer des données sensibles (p. ex : données concernant un patient) sur des boîtes mails privées personnelles de collaborateurs de manière non sécurisé. En cas de nécessité, seul un envoi sécurisé est toléré (« Guide d'utilisation HIN Secure Mail »).
- L'échange de données sensibles avec des partenaires externes ne peut se faire que par un réseau de mails sécurisés (réseau HIN ou « Guide d'utilisation HIN Secure Mail »).
- L'utilisateur est responsable de vérifier la source des mails qui lui sont adressés, la plus grande vigilance étant requise avant toute ouverture de pièces jointes ou de liens. En cas de doute, il peut contacter le Service Desk de l'HFR.
- Afin d'éviter les spams, l'utilisateur n'est pas autorisé à s'inscrire avec son adresse HFR sur des sites web privés sans lien avec l'activité professionnelle.
- Les propos tendancieux, diffamatoires, discriminatoires, violents et indécents sont interdits et ne peuvent par conséquent pas être diffusés par mail.

3.3 Logiciel et propriété intellectuelle

L'utilisateur, selon sa fonction et/ou son périmètre professionnel, se voit accordé l'accès à un ensemble de logiciels fourni par la DSIO. Les logiciels nécessitant des licences spécifiques payantes requièrent une validation du supérieur.

Tout logiciel doit être validé et fourni par la DSIO ou avec son accord. Un logiciel installé sans l'accord de la DSIO pourra être supprimé et aucun support ne sera fourni.

L'utilisation de logiciel sans licence appropriée et l'utilisation de copies de logiciel sont interdites.

3.4 Demande de support IT et prise à distance du poste

Seuls les utilisateurs de la Direction des systèmes d'information et opérations (DSIO), dans le cadre d'une demande de support sollicitée par un utilisateur, sont habilités à prendre le contrôle à distance d'un poste d'utilisateur, ceci avec l'approbation de ce dernier.
Toute demande de prise à distance d'un tiers sur un équipement de l'HFR sans l'accord d'un collaborateur DSIO doit être refusée.

3.5 Utilisation des comptes personnels et moyens d'authentification

L'utilisateur se voit attribuer un compte Windows personnel et, selon sa fonction, plusieurs comptes personnels dans des applications métiers.

Les comptes personnels, mots de passe et autres moyens d'authentification (p. ex. carte professionnelle de santé CPS, SMS, token, etc.) ne peuvent en aucun cas être transmis à des tiers (collègues ou personnes externes).

Ce principe est valable pour les comptes Windows et pour tous les comptes applicatifs spécifiques.

3.6 Utilisation de matériel/supports externes

L'utilisation de support externe sur son pc et laptop (p. ex : clé USB, disque dur externe, etc.) n'est pas tolérée pour des raisons de sécurité. Les éventuelles exceptions doivent être justifiées dans

une demande au service desk. La DSIO analysera les possibilités d'autorisations et se réservera le droit de refuser en cas de risque.

Les pc professionnels n'ont pas le Bluetooth activé par défaut. Si l'activation du Bluetooth sur le PC est souhaitée, une demande au service desk peut être faite mais la DSIO se décharge de toute responsabilité en cas d'incident de sécurité provoqué par une attaque à travers le Bluetooth.

3.7 Matériel privé et réseau

Aucun appareil privé (pc, laptop, smartphone, tablette, etc.) ne peut être branché sur le réseau filaire ni sur le wifi entreprise de l'HFR sans l'accord explicite de la DSIO.

Le stockage de documents professionnels et de données sensibles s'y rapportant est strictement interdit sur les appareils privés.

3.8 Accès VPN

L'accès depuis l'externe au SI HFR peut se faire avec un portable HFR et une solution Full VPN selon les besoins et les disponibilités en matériel de la DSIO.

L'accès est également possible depuis un poste privé à travers un portail Citrix. Le poste privé doit alors être sécurisé avec un antivirus et disposer d'un système d'exploitation à jour. Comme mentionné au point précédent, il est interdit de copier ou stocker des documents professionnels et des données sensibles sur le poste privé. L'HFR décline toute responsabilité pour les dommages causés suite à l'infection d'un poste privé par un malware.

3.9 Accès au DEP (dossier électronique du patient) *(NB : uniquement pour les collaborateurs disposant d'un tel accès)*

L'accès au DEP ne peut intervenir que par le biais d'un ordinateur HFR. L'accès au DEP depuis un poste privé, même par le biais d'un accès VPN Citrix, est strictement interdit selon les dispositions légales applicables au DEP.

L'accès au DEP peut donc intervenir uniquement depuis un poste HFR connecté au réseau local (filaire ou wifi) ou par le biais du Full VPN (NB : il faut un portable HFR).

En cas d'usage frauduleux du DEP au sein de l'institution, l'Association CARA, à laquelle l'HFR est affilié, se réserve le droit de suspendre ou résilier tout compte d'utilisateur sans préavis ni indemnité. L'Association CARA informe l'institution et l'utilisateur.

3.10 Impressions

Le système Equitrac (follow me printing) permet un contrôle des impressions comme précisé dans la Print Policy.

En règle générale, les collaborateurs impriment ou copient uniquement des documents en lien avec leur activité professionnelle. L'utilisation des multifonctions à titre privé n'est tolérée que si elle est minime en temps et en fréquence, qu'elle n'entraîne qu'une utilisation négligeable des ressources, qu'elle ne compromet ni n'entrave l'activité professionnelle, qu'elle ne relève pas d'une activité lucrative privée.

En cas d'abus, le collaborateur ainsi que son supérieur hiérarchique seront informés et une facture sera établie.

4 Devoirs de l'utilisateur

4.1 Devoir de confidentialité

Selon sa fonction, l'utilisateur se voit attribuer des accès, à des applications métiers contenant des données sensibles. Il a un devoir de confidentialité et est soumis à 2 secrets:

- Le secret de fonction qui couvre les faits dont il a eu connaissance dans l'exercice de ses fonctions qui doivent rester secrets en raison de leur nature, des circonstances ou d'instructions spéciales ;
- Le secret professionnel (ou secret médical) spécifique aux informations relatives à un patient.

Le secret de fonction et le secret professionnel perdurent au-delà de la fin des rapports de travail.

En cas de violation du devoir de fonction et du secret professionnel, des suites juridiques ou pénales sont réservées (art. 320 et 321 du code pénal suisse).

De manière générale, l'utilisateur n'est autorisé à consulter et à traiter que les données des patients avec qui il est en relation thérapeutique ou en cas de motif professionnel.

4.2 Respect des mesures de sécurité

L'utilisateur ne doit en aucun cas contourner les mesures de sécurité mises en place (p. ex : créer des wifi personnels, désactiver ou contourner des outils de sécurité du SI, etc.).

4.3 Annonce en cas d'incident de sécurité

L'utilisateur qui rencontre un incident de sécurité doit impérativement l'annoncer au Service Desk dans les meilleurs délais pour en limiter ses impacts.

4.4 Respect de la déontologie de l'HFR

Le stockage et la diffusion volontaire de données (images, vidéos, etc.) contraires à la déontologie de l'HFR sont strictement prohibés.

5 Mesures de contrôle et sanctions

Tous les accès à internet sont tracés et des contrôles peuvent être effectués (cf. RSF 122.70.17). Les accès aux réseaux internes, les accès aux applications métiers et l'utilisation des comptes informatiques peuvent également être contrôlés.

En cas de non-respect des règles définies du présent règlement, la DSIO se réserve le droit de couper ou restreindre les accès informatiques et l'utilisateur s'expose à des sanctions disciplinaires internes et/ou pénales selon la gravité des faits.

Le non-respect du secret de fonction ou professionnel expose le collaborateur à des poursuites pénales selon les articles 320 et 321 du code pénal suisse.

6 Adoption et entrée en vigueur

Le présent règlement a été adopté par le conseil de direction lors de sa séance du … .

Il entre en vigueur le 1er avril 2023

Fribourg, le 6 avril 2023

Marc Devaud
Directeur général

Stéphane Brand
Directeur des systèmes d'information et opérations