HÔPITAUX ROBERT SCHUMAN

Code de bonne conduite pour la sécurité de l'information au sein des Hôpitaux Robert Schuman à l'attention du personnel interne et externe

Table of Contents

Introduction

L'information médicale, soignante et administrative est soumise au strict respect d'obligations légales et déontologiques qui garantissent la sécurité et la protection des données relatives aux Patients et aux personnels exerçant au sein des Hôpitaux Robert Schuman (HRS).

1. OBJECTIFS DU CODE DE BONNE CONDUITE

Les objectifs prioritaires de ce code de bonne conduite sont :

- de responsabiliser le personnel et les partenaires médicaux et paramédicaux habilités aux risques liés à la sécurité de l'information
- d'informer les acteurs des HRS des bonnes pratiques de gestion de l'information dans un cadre légal et réglementaire
- de protéger les patients, les personnels internes et externes d'une violation de la sécurité de leurs données personnelles.

2. CHAMPS D'APPLICATION

Ce code de bonne conduite est applicable à toutes les personnes autorisées utilisant les systèmes de gestion de l'information des HRS (les utilisateurs).

Les utilisateurs peuvent être :

- Les membres du personnel des HRS,
- Les médecins salariés des HRS
- Les médecins libéraux agrées à la HRS
- Les autres personnels externes (consultants, etc.)

On entend par information, toute donnée relative au patient et ou au personnel intégrée dans le système d'information des HRS, orale et écrite sous format électronique *ou papier*.

- Les données relatives à la santé sont considérées par la loi comme des données sensibles*. À ce titre, les informations produites au sein de nos institutions, ne doivent être consultées que par les personnes habilitées à y accéder en raison de leurs fonctions."

- L'identification et l'authentification ont donc un caractère obligatoire dans le traitement confidentiel des données.

- Au regard de la loi, les Hôpitaux Robert Schuman ont **le droit** d'empêcher les **accès illégitimes aux données de santé à caractère personnel** contenues dans son système d'information.

** Annexe relative aux textes et règlements en vigueur au Luxembourg. Lire également l' Arrêté ministériel du 7 juillet 2005* ***approuvant le code de déontologie*** *des professions de médecin et de médecin dentiste édicté par le collège médical.*

Le système d'information comprend :

- **Les informations, orales, écrites sous format papier et électronique**
- **Les composants logiciels** (applications et bases de données mises à disposition des professionnels de santé),
- **les composants réseaux** (infrastructure Wifi ou réseaux physiques, câbles, etc.),
- **le poste de travail informatique physique** (écran, clavier, souris, unité centrale, imprimante, ordinateur portable).

3. RESPONSABILITE

Définition juridique du responsable du traitement :

La loi du 2 août 2002 précise que: est responsable du traitement, la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine **les finalités et les moyens du traitement** de données à caractère personnel. **HRS est responsable du traitement informatique des données sur son système d'information.**

Il est donc de la responsabilité de la direction des HRS **de garantir la sécurité des informations dont elle est la dépositaire** et de veiller au respect des règles d'utilisation des systèmes d'information mis en place et exploités par la Fondation.

Il est de la responsabilité de toute personne accédant aux et/ou utilisant les systèmes d'information des HRS de respecter les règles d'utilisation explicites de ce code de bonne conduite.

4. OBLIGATION DE SÉCURITÉ

La loi du 2 août 2002, précise dans son article 22(1) que tout responsable du traitement doit garantir la sécurité et la confidentialité des données.

Les obligations légales en matière de sécurité sont les suivantes :

- Le contrôle à l'entrée des installations (accès sécurisé)
- Le contrôle des supports (supports protégés)
- Le contrôle de la mémoire (restrictions d'accès aux systèmes d'administration)
- Le contrôle de l'utilisation (protection réseau (Firewalls, DMZ)
- Le contrôle de l'accès (gestion des comptes, suivi et administration)
- Le contrôle de la transmission (VPN, cryptage voire signature électronique)

- Le contrôle de l'introduction (login/mot de passe)
- Le contrôle du transport (cryptage des supports)
- Le contrôle de la disponibilité (backups/sauvegardes sécurisées)

5. LES BONNES PRATIQUES

- Les utilisateurs doivent déclarer au Service Desk tout incident de sécurité qu'ils détecteraient.
- Les utilisateurs doivent prendre toutes les précautions raisonnables pour protéger les informations qui leur sont confiées.
- Les utilisateurs sont responsables de leur environnement. Celui-ci sera maintenu propre, en ordre et sécurisé.
- Les utilisateurs ne sont pas autorisés à modifier la configuration des systèmes de gestion de l'information, ni leurs paramètres, mis à leur disposition par les HRS.
- L'accès à tous les systèmes de gestion de l'information doit être protégé.
- Les utilisateurs ont l'interdiction de divulguer leur mot de passe ou le cas échéant prêter leur carte d'authentification à puce à une tierce personne, y compris leur responsable ou leur assistant.
- Les utilisateurs sont responsables de la gestion de leur boîte à courriels.
- Il n'est pas autorisé, sauf autorisation explicite de transférer ou stocker des informations médicales issues du système d'information des HRS sur des mémoires de stockage de masse amovible (clés USB, CD-ROM, etc.).

6. SÉCURITÉ / MOTS DE PASSE

Tous les mots de passe doivent être renouvelés et adaptés conformément à la politique de sécurité des HRS.

7. DISCIPLINE

En cas de manquement à ce code de bonne pratique ou en cas d'infraction, l'utilisateur est passible de sanctions. La sanction sera adaptée à la gravité estimée de la faute en fonction du contexte et des législations en vigueur.
* *Annexe*

8. ENGAGEMENT

L'utilisateur déclare avoir pris connaissance du code de bonne conduite et s'engage à le respecter.

Nom : _____ Prénom : _____

Titre : _____

Signature : _____ Date : _____/_____/20___

9. ANNEXE RELATIVE AUX TEXTES DE LOI ET REGLEMENTS DE REFERENCE

Le traitement de données à caractère personnel en matière de surveillance du Courrier électronique, de l'utilisation d'Internet et du réseau informatique tombe dans le champ d'application de diverses dispositions légales qu'il convient de rappeler:

Toute modification du code de bonne conduite et toute mesure de surveillance doit être traitée au préalable au comité mixte. L'employeur, est dans l'obligation de demander une autorisation auprès de la CNPD.

- la Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après dénommée « Directive cadre »);

- la Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (ci-après dénommée «Directive vie privée et communications électroniques») ;

- l'article 8, alinéa (1) de la Convention européenne des Droits de l'Homme ;

- l'article 7 de la Charte des droits fondamentaux de l'Union européenne ;

- l'article 28 de la Constitution ;

- la loi du 28 août 1998 sur les établissements hospitaliers : art. 38 : droits des patients à la protection de leur vie privée ;

- la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après dénommée «la loi») ;

- la loi modifiée du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le Secteur des communications électroniques (ci-après dénommée «la loi du 30 mai 2005») ;

- la loi du 11 août 1982 concernant la protection de la vie privée (ci-après nommée « la loi du 11 août 1982 »);

- l'article 460 du Code pénal ;

- le Code du travail et notamment ses articles L.261-1, L.261-2 et L.423-1.

- Arrêté ministériel du 7 juillet 2005 approuvant le code de déontologie des professions de médecin et de médecin dentiste édicté par le collège médical.

- Le code de déontologie des professions de médecin et de médecin dentiste édicté par le collège médical art.4-6 sur le secret professionnel, les articles 44-50 sur l'information du patient et son consentement, et les articles 60-65 sur le dossier médical et les modalités du droit à son accès.

- Article 37, Annexe 8 „Liste des moyens informatiques et de télécommunication“ de la convention collective de travail

- Articles 15, 16, 18, 19, 20, 21 du Règlement grand-ducal du 07 octobre 2010 établissant le code de déontologie de certaines professions de santé