CODE DE CONDUITE DES UTILISATEURS

SÉCURITÉ ET CONFIDENTIALITÉ DE L'INFORMATION

JUIN 2020

CHU Sainte-Justine
Le centre hospitalier universitaire mère-enfant

Université de Montréal

CONTEXTE

Le code de conduite regroupe les principales normes et directives qui doivent être observées par tous les utilisateurs du Centre Hospitalier Universitaire Sainte-Justine « CHUSJ » qui ont accès ou qui gèrent des renseignements nominatifs à caractère confidentiel et personnel. Il indique le bon usage dans l'utilisation des actifs informationnels ainsi que la protection des données et des renseignements confidentiels.

OBJECTIFS

Ce code de conduite est un complément d'information à la Politique sur la sécurité de l'information du CHUSJ et à la Politique sur la confidentialité et l'accès au dossier de l'usager et vise à en faciliter l'application.
En outre, il a été conçu dans le but de respecter certaines mesures du cadre de gestion de la sécurité de l'information ainsi que les lois et directives gouvernementales en lien avec la protection des renseignements personnels et la sécurité de l'information.

DÉFINITIONS

ACTIF INFORMATIONNEL
Actif composé ou supportant de l'information, tel que système d'information, ordinateur, réseau de télécommunication, équipements médicaux spécialisés, documents se trouvant sur des supports tangibles ou intangibles (papier, matériel, logiciel, réseau) permettant son traitement, sa transmission ou sa conservation aux fins d'utilisation prévue.

CONFIDENTIALITÉ
Propriété d'une information de n'être accessible, ni divulguée qu'aux personnes ou entités désignées et autorisées. La diffusion d'information confidentielle pourrait porter préjudice à un usager ou un employé. Exemples : renseignements contenus au dossier de l'usager (nom, adresse, numéro de téléphone, courriel, résultats d'analyses ou d'examens, notes au dossier, plan de traitement, etc.) ou informations dites « privilégiées » (discussions, échanges verbaux, etc.).

DROIT À LA VIE PRIVÉE
Le droit à la vie privée est un droit fondamental protégé par la Charte des droits et libertés de la personne. Les renseignements contenus dans les dossiers d'usagers touchent au cœur de la vie privée des gens. La protection de la confidentialité de ces renseignements est essentielle au respect de la vie privée des usagers. Tout usager qui se présente au CHUSJ pour y recevoir des services de santé doit pouvoir confier des renseignements aux professionnels qui y œuvrent, dans un climat de confiance, où le respect du droit au respect de la vie privée de chacun est assuré.

RENSEIGNEMENT PERSONNEL
Tout renseignement portant sur un individu et qui permet de l'identifier est considéré comme un renseignement personnel, par exemple le nom et le prénom accompagnés de la date de naissance, le numéro d'assurance sociale, le numéro de permis de conduire, des renseignements de santé accompagnés du numéro de dossier etc. En général, les renseignements personnels sont confidentiels, sauf certaines exceptions prescrites par la loi.

TECHNOLOGIE DE L'INFORMATION
Tout logiciel ou matériel électronique et toute combinaison de ces éléments utilisés pour recueillir, emmagasiner, traiter, communiquer, protéger ou éliminer l'information sous toute forme (textuelle, symbolique, sonore ou visuelle).

UTILISATEUR
Toute personne qui accède ou utilise les actifs informationnels du CHUSJ, notamment les employés, les gestionnaires, les médecins, les dentistes, les pharmaciens, les professionnels de la santé, les travailleurs autonomes, les sous-traitants ou employés par un sous-traitant, les bénévoles, les résidents en médecine, les chercheurs, le personnel d'agences privées, les stagiaires, les étudiants, les contractuels et les fournisseurs.

RESPONSABILITÉ DES UTILISATEURS DES ACTIFS INFORMATIONNELS

CHAQUE UTILISATEUR :
- Prend connaissance de la Politique de sécurité de l'information, de la Politique sur la confidentialité et sur l'accès au dossier de l'usager et du Code de conduite. Les nouveaux employés y adhèrent en signant l'engagement de confidentialité;
- Est responsable de l'usage des ressources informatiques et du réseau auxquels il a accès;
- Est responsable du respect et de la protection de la confidentialité des renseignements contenus au dossier de l'usager;
- Informe rapidement son supérieur immédiat de tout incident susceptible de compromettre la confidentialité ou la sécurité de l'information;
- Contribue à la sécurité de l'information en adoptant un comportement éthique et approprié quant à l'utilisation des actifs informationnels;
- Est conscient que les actifs informationnels du CHUSJ sont réservés à un usage professionnel et dans le cadre de ses fonctions.

UTILISATION ÉTHIQUE DES TECHNOLOGIES DE L'INFORMATION

Les comportements appropriés et attendus par les utilisateurs des actifs informationnels du CHUSJ permettent d'assurer la disponibilité, l'intégrité, la confidentialité et la traçabilité de l'information. Pour ce faire, les actifs informationnels ne servent pas à :

- Créer, expédier ou réexpédier tout message électronique ou fichier susceptible d'affecter la sécurité et le fonctionnement de l'équipement mis à sa disposition;
- Utiliser à son profit, à des fins illégales ou inappropriées les actifs informationnels du CHUSJ;
- Visionner, télécharger, copier, partager ou expédier des images ou des fichiers au contenu à caractère érotique, présentant de la pornographie juvénile ou de la sexualité explicite ou à caractère diffamatoire, offensant, haineux, raciste, sexiste, violent;
- Écouter ou télécharger des émissions de radio ou de télévision en continu, sauf si requis dans le cadre de son travail;
- Écouter, télécharger des films ou de la musique, participer ou jouer à des jeux en ligne;
- Divulguer ou copier, sans autorisation, de l'information nominative sous quelque forme que ce soit;
- Consulter les informations contenues dans son propre dossier médical, l'employé doit se référer aux archives médicales

ACCÈS, DISCUSSION, COLLECTE ET ÉCOUTE D'INFORMATION CONFIDENTIELLE

Afin de préserver la confidentialité des renseignements personnels, il est strictement interdit de :
- Rendre publique des renseignements personnels et toute donnée provenant des dossier dossiers patients;

- Mentionner le nom d'un patient ou des renseignements susceptibles de l'identifier dans un lieu public (ascenseurs, cafétéria, corridors ou autres) et dans tout autre lieu où des personnes non autorisées pourraient l'entendre;
- Recueillir des informations ou d'accéder aux dossiers patients ou d'autres documents confidentiels, sous format papier ou numérique, si ce n'est pas requis dans le cadre de ses fonctions;
- Partager avec quiconque des renseignements personnels au sujet d'un patient ou d'un employé sans que cela ne soit requis dans le cadre de ses fonctions.

UTILISATION DES POSTES DE TRAVAIL ET DES SYSTÈMES D'INFORMATION

L'utilisation d'un poste de travail est un privilège accordé au personnel dans l'exercice de ses fonctions.

CHAQUE UTILISATEUR :
- Verrouille son poste de travail avant de s'absenter de son bureau (en utilisant simultanément les touches Windows+L ou Ctrl+Alt+Suppr), excepté pour les postes de travail ayant un code d'accès générique;
- Ferme tous les programmes informatiques ainsi que sa session et met en veille ou redémarre (et non éteint) son poste de travail à la fin de la journée afin que les sauvegardes puissent se faire régulièrement.

Afin de ne pas mettre à risque la sécurité des systèmes, il est strictement interdit :
- D'installer tout programme, logiciel ou autre composante sur un poste du CHUSJ, à moins d'en avoir l'autorisation;
- De copier des fichiers personnels (ex. : musique, vidéos, photos, etc.) sur son poste de travail ou sur un répertoire partagé;
- De brancher au réseau de télécommunication de l'établissement, tout poste de travail ou équipement qui n'appartient pas CHUSJ, à moins d'en avoir l'autorisation.

UTILISATION DES TERMINAUX MOBILES (portables, tablette, téléphone intelligent, etc.)

CHAQUE UTILISATEUR :
- Protège son ordinateur portable en le verrouillant avec un câble de sécurité, si disponible;
- Protège tous ses terminaux mobiles par un code d'accès privé;
- Prends les précautions nécessaires afin de garantir la sécurité des informations qu'il détient, lorsqu'il utilise ce type d'équipement;
- S'abstient de prendre des photos de documents confidentiels ou de transmettre des informations confidentielles à l'aide de son téléphone intelligent ou d'un autre support;
- Ne doit jamais sauvegarder des informations confidentielles sur un terminal mobile (ex. : sur le bureau, dans le répertoire Téléchargements ou sur une application de stockage, telle que Dropbox, Google Drive, etc.);
- Limite l'utilisation à son ordinateur portable à l'extérieur du CHUSJ puisque les filtres de sécurité sont inactifs, sauf si requis dans le cadre de son travail;
- Branche son portable au réseau de l'établissement, s'il n'est pas utilisé régulièrement, au moins une nuit par semaine pour effectuer une sauvegarde et faire les mises à jour;
- Range son portable hors de vue et hors d'accès lors de ses déplacements;
- Avise sans délai la Direction des ressources informationnelles et des technologies génie biomédicales (DRITGBM) de la perte ou du vol d'un équipement.

UTILISATION ET PROTECTION DES IDENTIFIANTS ET DES MOTS DE PASSE

CHAQUE UTILISATEUR :
- Est responsable des activités résultant de l'usage de son identifiant;
- Choisit judicieusement ses mots de passe afin qu'ils soient « sécuritaires » et « uniques » en ayant un minimum de 8 caractères dans 3 ou 4 de ces catégories, selon les limites du système:
  - chiffres (0 à 9); lettres MAJUSCULES; lettres minuscules;
  - caractères spéciaux (+, -, /, $, %, ? *, &, !, », «, etc.)
- S'assure de ne pas partager ou de rendre accessible son identifiant et ses mots de passe en s'abstenant de les écrire dans son agenda, sur une note autocollante ou un papier à proximité de son ordinateur. Si possible, il les conserve dans un endroit sécurisé tel un gestionnaire de mot de passe.

UTILISATION DU COURRIER ÉLECTRONIQUE

CHAQUE UTILISATEUR :
- Se connecte exclusivement à Microsoft Outlook (O365) pour ses communications reliées au travail;
- Ne transfère pas de documents confidentiels vers sa boîte courriel personnelle;
- S'identifie en tant qu'expéditeur en incluant dans sa signature : son nom, son titre d'emploi, ses coordonnées et son numéro de téléphone;
- Est vigilant, s'abstient d'ouvrir et de supprimer tout courriel contenant des titres accrocheurs (hameçon) uniquement en anglais, ayant un sujet inhabituel ou contenant des liens ou pièces jointes dont il ne connaît pas la provenance. Dans le doute, il informe le CSDT;
- Privilégie l'utilisation de son courriel corporatif pour ses communications professionnelles.

UTILISATION D'INTERNET

Étant donné que la confidentialité est souvent compromise dans le réseau Internet et que son utilisation est une source importante de programmes malveillants pouvant mettre à risque nos systèmes,

CHAQUE UTILISATEUR :
- Restreint son utilisation d'Internet qu'à des fins professionnelles;
- S'abstient de sauvegarder ou de diffuser des informations relatives au travail sur Internet (ex. : site de stockage, de transfert de fichiers, réseaux sociaux);
- Évite de télécharger ou d'envoyer des fichiers de grande taille (plus de 200 Mo ou 0,2 Go) ou si requis, planifie l'envoi avant 8 h et après 16 h.

UTILISATION DES RÉSEAUX SOCIAUX (facebook, linkedin, Twitter, Youtube, etc.)

CHAQUE UTILISATEUR :
- Est conscient du caractère public de ce qui est publié sur les réseaux sociaux et évite d'y mettre tout contenu pouvant porter préjudice ou atteinte à la réputation de l'établissement, d'un collègue, d'un gestionnaire, d'un usager ou de ses proches;
- S'abstient de naviguer sur les réseaux sociaux à partir de son poste de travail, sauf si requis dans ses fonctions;
- S'abstient d'utiliser les sites de lecture vidéo tel que YouTube ou autres pour écouter de la musique ou des vidéos, sauf si requis dans ses fonctions.

UTILISATION ET CONSERVATION DES MÉDIASAMOVIBLES (clé USB, CD, téléphone intelligent, etc.)

CHAQUE UTILISATEUR :
- Restreint la connexion de médias amovibles à un ordinateur du CHUSJ que pour un usage professionnel seulement;
- Privilégie l'utilisation d'outlook pour l'échange de fichiers à l'extérieur de l'établissement;
- Utilise une clé USB chiffrée lorsque les autres mécanismes de communication ne sont pas disponibles (ex. : fichier trop volumineux pour l'envoi d'un courriel);
- S'abstient de déposer des informations sensibles ou confidentielles sur un média amovible non chiffrée. Si requis et autorisé par son supérieur, il conserve ce média sous clé (ex. : classeur verrouillé) à l'intérieur du CHUSJ.

UTILISATION ET MANIPULATION DES DOCUMENTS PAPIERS

CHAQUE UTILISATEUR :
Chaque utilisateur qui possède, accède, manipule des documents papier, de même que tout dossier d'usager, tout document comportant des renseignements cliniques relatifs à un usager, qu'il se trouve dans un lieu clinique, une unité de soins, un bureau de professionnel ou tout autre emplacement, doit s'assurer:
- De la protection de la confidentialité des renseignements contenus au dossier de l'usager ou de l'employé et du droit fondamental de chacun au respect de sa vie privée;
- S'abstenir de prendre connaissance de tout document qui ne lui est pas destiné ou non requis dans le cadre de ses fonctions;
- S'abstenir de jeter des documents confidentiels qui ne sont plus utiles dans une poubelle, mais plutôt en utilisant une déchiqueteuse ou en les plaçant dans des bacs de déchiquetage verrouillés;

Note : Tous les éléments de dossier produits par les professionnels (ex : notes, rapports, etc.) qui n'ont pas encore été versés au dossier doivent être conservés dans des lieux sécurisés, accessibles aux seules personnes autorisées.

TÉLÉTRAVAIL

CHAQUE UTILISATEUR :
- Adopte un comportement sécuritaire similaire à celui adopté lors de sa présence physique au bureau. Il est important de faire attention à son environnement physique;
- Maintient la vigilance (rappelez-vous que vous êtes la première ligne de défense de l'organisation contre les cyberattaques);
- S'abstient de sauvegarder sur son appareil personnel des documents confidentiels;
- Protège son ordinateur portable personnel avec une solution antivirale à jour;
- S'assure que les versions les plus récentes du système d'exploitation, navigateur et applications sont installées;
- Ne tient aucune conversation confidentielle en présence de tierces personnes, et protège tout document contenant des renseignements confidentiels, qu'il s'agisse de documents en format papier ou numérique, afin que ceux-ci ne soient pas accessibles à des tiers.