Centre intégré
de santé
et de services sociaux
de la Montérégie-Ouest
Québec

Guide des bonnes pratiques en sécurité des ressources informationnelles

---

Document émis par la Direction des ressources informationnelles de la Montérégie

Version 1,7

30 octobre 2020

Contexte

La sécurité de l'information clinique, médicale, clinico-administrative et administrative de notre établissement fait partie de notre réalité quotidienne et nos comportements éthiques et sécuritaires sont des éléments majeurs de la solution face aux différentes menaces. Afin d'adopter ou de réaffirmer les bonnes pratiques sur l'utilisation des actifs informationnels, voici quelques principes que nous devons tous appliquer, quels que soient nos secteurs d'activités ou nos fonctions.

De nos jours, il y a une montée fulgurante des cyberattaques et de nombreuses organisations ont été des victimes de ces cyberfraudes et cyberattaques. La menace vient de partout sur le globe, et le réseau et le domaine de la santé ne sont pas épargnés. Un incident peut survenir en tout temps, il faut donc contribuer dès maintenant à la prévention et à la protection de nos informations. N'attendons pas qu'un incident grave dans notre établissement porte préjudice à nos usagers.

La sécurité de l'information, c'est l'affaire de tous!

Que voulons-nous sécuriser en particulier ?

- Les renseignements personnels et médicaux d'un patient ou tous renseignements considérés confidentiels pour l'établissement, par exemple :
  - Les diagnostics médicaux;
  - Les résultats de laboratoire, les informations sur les allergies alimentaires, les informations sur la pharmacologie, l'imagerie et le psychosocial, sans oublier nos secteurs jeunesse et nos établissements régionaux;
- Les renseignements combinés permettant d'identifier physiquement un usager/patient (date de naissance, numéro d'assurance-maladie, numéro de dossier, nom/prénom, etc.);
- Les renseignements du dossier d'employé (numéro d'assurance sociale, prélèvement de pension alimentaire, dossier disciplinaire, etc.);
- Les ordinateurs et serveurs;
- Les médias de stockage mobiles lorsque jugés nécessaires par le détenteur des actifs informationnels (clés USB, disques durs externes, etc.);
- Les médias de sauvegarde.

En bref, toute information sur les personnes et toute information confidentielle ou critique détenue par notre établissement ou sous sa responsabilité.

Médias de stockage mobiles

- La DRIM recommande d'éviter l'utilisation des clés USB et autres médias amovibles, afin de prévenir la perte, le vol ou la fuite de données;
- Toujours privilégier les transferts d'information par les systèmes d'information sécuritaires en place, ou sinon par les outils collaboratifs sécurisés du MSSS;
- Les utilisateurs sont responsables des données stockées sur les médias amovibles, en particulier les données confidentielles (nominatives, personnelles, médicales ou sensibles);
- Ne jamais copier de renseignements personnels et médicaux d'un patient ou confidentiels pour l'établissement sur un média amovible non protégé, dans le but de transmettre de l'information autant à l'interne qu'à l'externe de nos installations;
- Ne pas laisser un média amovible librement sur votre espace de travail : celui-ci doit être placé dans un lieu sûr et sécuritaire (ex. : mis sous clé dans un tiroir ou un classeur);
- Ne pas utiliser de média amovible fourni par l'établissement pour des besoins personnels ou sur vos ordinateurs personnels;
- Ne pas utiliser de média amovible personnel sur les ordinateurs appartenant à l'organisation;
- Ne pas copier de fichiers illégaux ou de source non sûre sur tout média amovible, afin d'éviter la propagation de virus;
- Chaque média amovible sur lequel sont stockées des données confidentielles doit contenir un mécanisme de protection contre l'accès non autorisé ou de copie (par exemple : un cryptage avec mot de passe).

Information sur un support papier

- Récupérer un document imprimé immédiatement après son impression;
    - Appliquer la même pratique pour les télécopies;
    - Utiliser l'impression sécurisée, lorsque disponible, notamment sur les imprimantes multifonctions;
- Protéger adéquatement un document contenant des renseignements sensibles ou confidentiels (par exemple : enveloppe sécurisée, cachetée, etc.) lors d'un envoi par courrier interne/externe ou par la poste;
- Sécuriser physiquement les documents papier dans un lieu sûr et sécuritaire (par exemple : tiroir, classeur barré, etc.);
- Disposer des documents ou de tout type de médias de copie (ex. : copie conforme papier) dans un bac verrouillé « confidentiel » prévu à cet effet et non dans la récupération régulière ou dans les corbeilles pour le papier.

Systèmes d'information

- Utiliser un compte nommé (et non un compte générique) pour accéder aux systèmes d'information, afin d'assurer la traçabilité de l'information;
- Lors de la création des droits d'accès d'un employé, les pilotes de systèmes d'information doivent appliquer le principe du moindre privilège selon les fonctions de l'employé;
- Réviser les accès lors des changements de fonctions des employés;
- Supprimer les accès lors de départs d'employés;
- Toujours verrouiller ou fermer l'accès à un système d'information dès que l'on quitte son ordinateur (que ce soit pour aller chercher un café ou aller en pause);
- Utiliser un jeton pour un accès à distance sécurisé aux applications informatiques du RSSS lors de télétravail et pour des activités administratives et cliniques.

Prévenir les fuites de données confidentielles

- Ne jamais partager ou laisser à la vue les données d'identification (nom d'utilisateur) et d'authentification (mot de passe), par exemple : pas sur des « Post-it », pas sur un petit papier sous le clavier et pas dans l'agenda situé sur votre bureau;
- Ne pas distribuer de rapports/fichiers/données sauf aux destinataires dûment autorisés;
- Ne jamais communiquer de données provenant des systèmes d'information fournis et utilisés par l'organisation (par exemple : pas par photo, cellulaire, Facebook, messagerie, etc.);
- Éviter toute extraction de données et les consulter exclusivement dans les applications prévues à cet effet;
- Verrouiller votre session dès que vous vous éloignez de votre poste de travail;
- Fermer votre session applicative sur un ordinateur partagé dès vous ne l'utilisez plus.

Destruction sécuritaire de l'information TI

- Lors de la suppression d'un fichier ou des courriels sur votre ordinateur, le fichier ou les courriels ne sont pas éliminés par défaut dans la corbeille; il faudra vider régulièrement la corbeille de l'ordinateur;
- Pour la disposition de clés USB ou de CD/DVD/VHS/Cassettes audio qui pourraient contenir des renseignements sensibles ou confidentiels, veuillez retourner le tout à la DRIM et nous verrons à faire détruire le contenu de façon sécuritaire;
- Lors du départ d'un employé, la DRIM a la responsabilité de récupérer son ordinateur et de le reconfigurer avant une nouvelle utilisation ou avant de le remettre à un autre employé;

- Ne jamais récupérer ou s'approprier le matériel informatique de l'organisation, même si celui-ci n'est plus fonctionnel ou a atteint sa fin de vie utile; la DRIM a la responsabilité d'assurer la destruction sécuritaire du contenu (données).

Journalisation des accès, surveillance et enquête

- Les accès de plusieurs actifs informationnels sont journalisés, par exemple les applications comme i-CLSC, la navigation sur l'Internet, le système de messagerie provincial, entre autres;
- Sur demande de la DRHCAJ (incluant les affaires juridiques), du CMDP ou encore du bureau du commissaire aux plaintes, la DRIM peut effectuer des extractions de données provenant de la journalisation pour confirmer des accès non autorisés d'un utilisateur (qu'il s'agisse d'un employé, d'un professionnel, d'un bénévole, d'un stagiaire, d'une main-d'œuvre indépendante ou de tout autre utilisateur autorisé);
- Les demandes d'accès aux journaux doivent être acheminées par le conseiller en relations de travail au conseiller-cadre à la sécurité des ressources informationnelles régionales;
- L'accès aux données de journalisation est réservé aux personnes autorisées et à hauts privilèges, selon le profil distinct ou limité.

Les outils de collaboration du MSSS (Outlook, Teams, Sharepoint, OneDrive Enterprise et autres outils disponibles sur la plateforme en ligne de l'établissement)

- Suivre les recommandations du MSSS pour l'utilisation éthique et sécuritaire des outils collaboratifs, incluant le système de messagerie provincial mis à la disposition des utilisateurs du RSSS (voir les « Termes et conditions d'utilisation des outils de collaboration », disponible sur la plateforme en ligne);
- Les outils de collaboration offerts par le MSSS répondent aux exigences ministérielles et gouvernementales de sécurité de l'information. Les utilisateurs sont donc tenus d'utiliser, dans le cadre de leurs fonctions, les outils de collaboration fournis par le MSSS et d'en adopter un usage exemplaire, au regard des dispositions du cadre de gouvernance de la sécurité de l'information et des meilleures pratiques en la matière;
- Les outils de collaboration ne doivent aucunement se substituer aux processus d'affaires en place, ils viennent compléter l'offre de services ministérielle en matière de technologies de l'information. Les systèmes d'information en place doivent donc être utilisés en priorité lorsque disponibles.

Le système de messagerie provincial (SMÉ – Courriel)

- Afin d'assurer la sécurité de votre compte de messagerie, vous devez :

    - Vérifier si vous connaissez l'expéditeur du courriel;
    - Vérifier si le contenu du courriel est relié à votre travail;
    - Si le courriel est « douteux » ou non sollicité :
        - **Signaler le courriel comme « indésirable » * ;**
        - Ensuite, vous pouvez supprimer le courriel simplement;
        - Ne pas ouvrir les pièces jointes;
        - Ne pas cliquer sur les hyperliens;
        - Ne pas répondre à l'expéditeur;
        - Ne pas faire suivre ledit courriel sauf à une ressource de la DRIM sur demande;
        - * Solliciter la collaboration de la DRIM en cas de doute quant à la légitimité d'un courriel;
- Ne pas utiliser les groupes d'envoi généraux des organisations pour l'envoi de courriels, ces groupes sont à l'utilisation exclusive du service des communications;
- Ne pas utiliser la fonction « Répondre à tous » pour répondre à l'expéditeur lorsqu'un envoi a été fait par erreur ou lorsque non nécessaire.

Règles d'un bon mot de passe :

- **Meilleur choix :** avoir un mot de passe plus long lorsque c'est possible;
    - Utiliser des phrases au lieu de mots pour un mot de passe :
        - ✓ Par exemple : Bonneetheureuseannée2020santeetbonheur
        - ✓ Exemples plus courts lorsque le nombre de caractères est restreint : Jemangebio, jaimecourir, jesuismatinale, Jaineufcousines;
- Si le nombre de caractères est très restreint, utiliser trois des quatre types d'éléments suivants : minuscule, majuscule, chiffre et symbole;
- Ne pas utiliser certains mots de passe qui sont répertoriés comme non sécuritaires :
    - Liste des pires mots de passe 2019
        - ✓ Par exemple, référence suivante : https://ici.radio-canada.ca/nouvelle/1442392/pires-mots-de-passe-2019-liste-splashdata;
- Ne jamais donner son mot de passe à une autre personne (ex. : ni à son gestionnaire, ni à un collègue de travail, ni même à un employé ou fournisseur lors d'appels de soutien);
- Ne jamais utiliser le même mot de passe pour accéder à plusieurs systèmes d'information; employer un mot de passe distinct par système d'information.

Comment bien utiliser l'Internet

- Utiliser l'Internet lorsque nécessaire pour réaliser les tâches liées à ses fonctions;
- Valider **si un site est sécuritaire avant d'y accéder**, au besoin, consulter le Centre de soutien informatique;
- Ne pas utiliser l'Internet pour des besoins personnels ou commerciaux;
- Ne pas diffuser des renseignements personnels, confidentiels ou sensibles sur les services infonuagiques **publics** (par exemple : Google Drive, Dropbox, etc.);
- Utiliser en priorité les outils de collaboration du MSSS fournis par l'établissement;
- Ne pas diffuser ou communiquer d'informations personnelles, confidentielles ou sensibles sur l'Internet, à l'exception des systèmes d'information du réseau de la santé.

Si une fenêtre apparaît à l'écran vous informant que vous avez un virus

- Fermer votre ordinateur;
- Débrancher le fil de réseau relié à votre ordinateur;
- Aviser le centre d'assistance de la DRIM;
- Prendre des notes sur ce qui a mené à l'infection de votre ordinateur;
- Collaborer avec la DRIM dans la prise en charge de l'incident.

POUR TOUTE QUESTION SUR LA SÉCURITÉ :

envoyer une requête au système de billetterie de votre Centre de soutien informatique.

Éthique de l'utilisation des technologies de l'information

Selon la directive de sécurité sur l'utilisation éthique des technologies de l'information[1], un membre du personnel ou tout autre utilisateur autorisé, **NE DOIT JAMAIS** utiliser les technologies de l'information mises à sa disposition pour :

- Harceler un autre membre du personnel de la fonction publique ou toute autre personne;
- Visionner, télécharger, copier, partager ou expédier des images ou des fichiers érotiques, de pornographie juvénile ou de sexualité explicite, ou dont le contenu a un caractère diffamatoire, offensant, harcelant, haineux, violent, menaçant,

[1] http://extranet.ti.msss.rtss.qc.ca/getdoc/cf73b86c-46be-48b4-907a-779ba1162bc7/MSSS05-005-Directive-sur-l-utilisation-ethique-des.aspx

raciste, sexiste, ou qui contrevient à l'une des dispositions de la Charte des droits et libertés de la personne (L.R.Q., c. C-12), ainsi que de toute autre loi au Québec;

- Télécharger tout logiciel ou partager ou copier un logiciel installé sur l'équipement gouvernemental auquel il a accès sans une autorisation préalable;
- Télécharger des émissions de radio ou télévision en continu;
- Télécharger des films ou de la musique;
- Utiliser à son profit les TI mises à sa disposition;
- Créer, expédier ou réexpédier tout courriel, message ou fichier qui contient un élément qui contrevient aux paragraphes qui précèdent;
- Créer, expédier ou réexpédier tout courriel, message ou fichier qui est susceptible d'affecter le fonctionnement de l'équipement mis à sa disposition ou d'un réseau gouvernemental auquel il est relié, ou d'engendrer des coûts additionnels à l'employeur;
- Exercer des moyens de pression ou soutenir de tels moyens à des fins de manifestation ou d'incitation à des manifestations;
- Nuire à la prestation de travail d'un autre membre du personnel;
- Participer, regarder ou jouer à des jeux en ligne;
- Utiliser les équipements TI pour des activités illégales ou malhonnêtes;
- Accéder à des informations non nécessaires à l'exécution normale de son travail.