Ministère de la Santé
et des Services sociaux

Technologies de l'information

DIRECTIVE

MSSS-DIR04

Directive sur l'utilisation sécuritaire des outils de collaboration par les médecins

Version : 1.0

Approuvé par: *Luc Bouchard, sous-ministre associé et dirigeant de l'information*

Mise en vigueur: *xxxx-xx-xx*

Québec

Cette page est laissée intentionnellement vide.

Préambule

La présente directive est définie par le dirigeant réseau de l'information du réseau de la santé et des services sociaux (RSSS) dans le cadre de la gouverne du système de santé québécois.

Dans le cadre des orientations gouvernementales visant une utilisation efficace et efficiente des technologies de l'information, le ministère de la Santé et des Services sociaux (MSSS) offre aux médecins, résidents et externes (étudiants en médecine), une panoplie d'outils de collaboration à usage professionnel, leur permettant ainsi d'accroitre leurs capacités de collaboration.

Une vigie menée auprès d'institutions gouvernementales d'autres juridictions, comparables au Québec, révèle que celles-ci intègrent au sein de leurs systèmes de courriel, tout intervenant manipulant des données de santé, c'est le cas notamment du Royaume-Uni avec NHSmail.

Le niveau de sécurité des outils de collaboration acquis par le MSSS, incluant le système de messagerie corporatif, a été rehaussé afin de répondre notamment aux besoins d'échanges et de partage de données confidentielles.

La directive vise à garantir l'adhésion de ce corps d'emploi puisque ce dernier s'est récemment vu octroyer des comptes Office 365. Les autres professionnels de la santé sont également assujettis aux mêmes conditions véhiculées dans d'autres documents d'encadrement.

Le MSSS, par le biais de son ministre, demeure le dépositaire des données de santé et sociales de ses usagers. Il doit veiller à leur sécurité tout au long de leur cycle de vie.

Objectif

La présente directive a pour objectif d'encadrer l'utilisation sécuritaire des outils de collaboration, notamment le système de messagerie corporatif au sein des établissements publics, particulièrement par les médecins, les résidents et les externes. Le but étant de préserver le système de santé du Québec contre toute atteinte à la disponibilité, à l'intégrité et à la confidentialité des informations dont ils disposent.

Champ d'application

1. Cette directive s'applique aux :

   1° MSSS;

   2° Organismes publics visés au paragraphe 5 de l'article 2 de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03) [1];

   3° Médecins[2], résidents et externes (étudiants en médecine).

Documents d'encadrement connexes

2. Ce document précise certaines exigences en sécurité de l'information et s'inscrit dans une perspective globale incluant notamment[3] :

[1] http://legisquebec.gouv.qc.ca/fr/ShowDoc/cs/G-1.03

[2] Tout médecin dont la prestation de service s'effectue en établissement ou pour le compte d'un établissement

1° La Politique provinciale de la sécurité de l'information – MSSS-POL01;

2° Le Cadre de gestion de la sécurité de l'information – MSSS-CDG01;

3° La Règle particulière sur la sécurité organisationnelle;

4° La Directive sur la déclaration des incidents de sécurité – MSSS-DIR01;

5° Les conditions d'utilisation des outils de collaboration[4];

6° Le cadre de gouvernance de la sécurité de l'information de l'établissement.

3. La sécurité de l'information à un niveau organisationnel étant considérée comme un ensemble, les exigences de sécurité spécifiées dans les divers documents d'encadrement de la sécurité de l'information s'additionnent et se complètent.

Définitions

4. Dans la présente directive, on entend par :

1˚ **Actif informationnel** : une banque d'information, un système d'information, un réseau de télécommunication, une infrastructure technologique ou un ensemble de ces éléments ainsi qu'une composante informatique d'un équipement médical spécialisé ou ultraspécialisé.
Est également considéré comme un actif informationnel, tout support papier contenant de l'information.

2˚ **Cycle de vie de l'information** : L'ensemble des étapes que franchit une information et qui vont de sa création, en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation ou sa destruction, en conformité avec le calendrier de conservation du MSSS.

3˚ **Données confidentielles** : Information qui ne peut être communiquée ou rendue accessible qu'aux personnes et aux entités autorisées.
On parlera plus spécifiquement d'information sensible lorsqu'une information confidentielle a le potentiel de mettre en péril l'intégrité de la personne ou de l'organisation qu'elle concerne.
Les données personnelles, médicales, sociales des usagers ainsi que les données de recherches et administratives sensibles sont considérées comme des données confidentielles.

5. Les outils de collaboration acquis par le MSSS se déclinent comme suit :

1˚ **Outlook** : Système de messagerie, calendrier, planificateur de tâches, etc.;

2˚ **OneDrive Entreprise** : Stockage des fichiers professionnels personnels;

3˚ **SharePoint Online** : Partage et gestion de contenu;

4˚ **Microsoft Teams** : Échange instantané d'informations et de fichiers. Visioconférence et clavardage, etc.;

---

[3] http://extranet.ti.msss.rtss.qc.ca/Orientations-et-gouvernance/Securite/Cadre-normatif.aspx
[4] https://msss365.sharepoint.com/sites/MSSS-Collaboration-SPO/SitePages/Orientations.aspx

5˚ **Microsoft Forms** : Enquêtes et sondages;

6˚ **Sway** : Création et partage des rapports, présentations, récits personnels interactifs;

7˚ **Power Automate** : Création de flux de travaux entre les applications, les fichiers et les données;

8˚ **Office 365 MyAnalytics** : Analyse des données pour une meilleure productivité;

9˚ **Microsoft Planner** : Gestionnaire de projet;

10˚ **Microsoft Stream** : Partage de vidéo, de présentations et de réunion, Office 365, SharePoint.

Obligations des médecins, résidents et externes

6. Tout médecin, résident ou externe a l'obligation de protéger les actifs informationnels mis à sa disposition par le MSSS ou le RSSS. À cette fin, il doit :

   1˚ Adhérer à la solution corporative des outils de collaboration, dont le système de messagerie;
   2˚ Utiliser exclusivement son compte corporatif MSSS, pour tous ses échanges de données confidentielles;
   3˚ Appliquer une couche de chiffrement supplémentaire, approuvé par le MSSS ou le RSSS, lorsque le médecin, résident ou l'externe échange des données confidentielles avec un destinataire externe à la plateforme de collaboration corporative;
   4˚ Délaisser l'utilisation des autres systèmes de messagerie publics pour ses échanges de données concernant les usagers;
   5˚ Éviter de contourner l'utilisation du système de messagerie corporatif par le biais de redirections automatiques de courriels ou tout autre mécanisme de contournement[5].

Échange des données confidentielles

7. Tout médecin, résident ou externe, ne doit pas recourir aux outils de collaboration à des fins d'échanges d'informations confidentielles[6], concernant un usager, s'il existe des processus d'affaires validés par les médecins et prévus à cet effet. En cas d'absence de tels processus d'affaires, le MSSS autorise l'utilisation des outils de collaboration à cette fin.

Déclaration d'un incident

8. Tout médecin, résident ou externe, doit signaler immédiatement au centre de services de l'établissement, dont il relève, tout acte dont il a connaissance, susceptible de constituer une violation réelle ou présumée des règles de sécurité ainsi que toute anomalie pouvant nuire à la protection des actifs informationnels du MSSS ou RSSS, en vertu de la directive sur la déclaration des incidents[7].

---

[5] Consulter le Guide des téléconsulations du MSSS pour plus de précisions : https://telesante.quebec/.
[6] Une information confidentielle est définie comme étant une information à caractère personnel, médical, social ou toute autre information que l'organisation considère comme telle.
[7] MSSS-DIR01 Déclaration des incidents de sécurité - 2015-08-17

Obligation des établissements et organismes RSSS

9. Tout établissement ou organisme visé à l'article 2 doit :

    1° Mettre en œuvre la présente directive;
    2° Sensibiliser son personnel médecins, résidents et externes à la sécurité de l'information;
    3° Offrir le soutien de premier niveau auprès des médecins, résidents et externes concernant notamment la création des comptes;
    4° Bloquer, par des mécanismes de filtrage web, les sites de messageries publics[8] ou tout autre outil de collaboration non autorisé sur le réseau informatique des établissements.

Sanctions

10. Lorsqu'un médecin, résident ou externe contrevient à la présente directive, il s'expose à des mesures disciplinaires, administratives ou légales, en fonction de la gravité de son geste. Ces mesures peuvent inclure la suspension des privilèges, la réprimande, la suspension, le congédiement ou autre, et ce, conformément aux règles en vigueur.

11. L'établissement du RSSS ou le MSSS peut transmettre à toute autorité judiciaire les renseignements colligés et qui le portent à croire qu'une infraction à toute loi ou règlement en vigueur a été commise.

Droit de regard

12. Le MSSS exerce, en conformité avec la législation et la réglementation en vigueur, un droit de regard sur tout usage de ses actifs informationnels. L'utilisation des outils de collaboration par les médecins, résidents et les externes, ne fait pas exception.

Dispositions finales

13. Le dirigeant de l'information se réserve le droit de requérir d'un établissement ou d'un organisme une preuve du respect de la directive en tout temps.

14. L'ensemble des éléments de la présente directive devra faire l'objet d'une reddition de compte au dirigeant de l'information minimalement dans le bilan de sécurité de l'information chaque année.

15. La présente directive a été approuvée par le dirigeant réseau de l'information le : 12 novembre 2020

16. La présente directive entre en vigueur le : 4 décembre 2020

[8] Gmail, Hotmail et Yahoo Mail, etc.