Ministère de la Santé et des Services sociaux

Direction générale des technologies de l'information

Utilisation sécuritaire des données patients

27 octobre 2020

Votre gouvernement

Québec

Plan de la présentation

1. Contexte
2. Consultations
3. Portée de la directive
4. Sommaire des exigences
5. État de situation
6. Aide-Mémoire
7. Prochaines étapes

Québec

1. Contexte

- Utilisation persistante du courriel privé, grand public, à des fins professionnelles (absence totale de sécurité)
- Enjeu soulevé à maintes reprises par les directeurs des ressources informationnelles (DRI) et les responsable de la sécurité de l'information (RSI) du réseau de la santé et des services sociaux (RSSS) quant à l'utilisation, notamment par les médecins, d'outils dépourvus de sécurité et d'encadrement du ministère de la Santé et des Services sociaux (MSSS) ou du RSSS
- Situation problématique amplifiée par le télétravail
- Incidents de sécurité à répétition, dus principalement à des manipulations hasardeuses de l'information confidentielle des usagers
- Radiation temporaire par le collège des médecins de certains médecins ayant fait mauvais usage des données confidentielles des usagers
- Inquiétudes soulevées par le Secrétariat du Conseil du trésor
- **Recommandation de mettre en œuvre une obligation quant à l'utilisation des outils « santé » par les médecins.**

Québec

2. Consultations

- Atelier de travail tenu le 10 février 2020 pour échanger sur la problématique et tracer les grandes lignes (M. Dave Roussy, Mme Agathe Tremblay, M. François Bérubé, M. Yvan Fournier, Mme Sarah Bouchard, M. Sergio Fernandes, M. Jean Boulanger)
- Pertinence d'élaborer une directive sur l'utilisation sécuritaire des outils de collaboration spécifiquement pour les médecins
- Consultations menées auprès d'autres DRI et RSI sur le contenu de la directive
- Ateliers techniques avec la Direction générale adjointe des opérations technologiques, Direction générale adjointe de la transformation numérique et de la planification et la Direction générale adjointe de la cybersécurité et de l'intelligence artificielle
- Consultation du comité d'orientation de la Direction générale des technologies de l'information
- Consultations élargies à la Direction générale des affaires universitaires, médicales, infirmières et pharmaceutiques, au Collège des médecins, à la Fédération des médecins spécialiste du Québec (FMSQ) et à la Fédération des médecins omnipraticiens du Québec (FMOQ)
- Présentation au comité des ressources informationnelles du RSSS

Québec

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

Québec

3. Portée de la directive

Concerne :

- Médecins, résidents et médecins spécialistes (dont la prestation de service s'effectue en établissement ou pour le compte d'un établissement)
- Externes, étudiants en médecine

S'applique à l'ensemble des outils de la suite Office 365 :

- Outlook
- OneDrive Entreprise
- SharePoint Online
- Microsoft Teams
- Microsoft Forms
- Microsoft Planner
- Microsoft Stream
- Etc.

Québec

4. Sommaire des exigences

- **Obligations des médecins**
  - Seuls les outils de collaboration MSSS doivent être utilisés pour les échanges de données confidentielles (médicales, sociales, etc.)
  - Interdiction des redirections automatiques de courriels
  - Les outils d'Office 365 ne doivent pas se substituer aux processus d'affaires ni aux applications cliniques où l'échange de données confidentielles est déjà prévu

Québec

4. Sommaire des exigences (suite)

- **Obligations des établissements**
  - Sensibiliser ce corps d'emploi
  - Offrir le soutien de premier niveau, notamment lors de la création et la gestion de compte
  - Blocage d'accès aux sites de messageries publiques, Gmail, Hotmail et Yahoo Mail par filtrage web

Québec

5. État de situation

- Déploiement des Termes et Conditions d'utilisation des outils de collaboration corporatifs Office 365 (En cours d'approbation)
- Élaboration d'une directive sur l'utilisation sécuritaire des outils de collaboration par les médecins (*sous réserve d'approbation*)
- Création de comptes à l'ensemble des médecins pratiquant en établissements
- Plusieurs nouveaux services exigent que les médecins possèdent et utilisent un compte Office 365 Santé
    - Service Téléfax : 296 médecins spécialistes
      134 médecins omnipraticiens
      8 médecins résidents
- Position favorable du collège des médecins, la FMSQ et la FMOQ
- Élaboration d'un document d'aide mémoire pour l'ensemble des médecins

Québec

5. État de situation (suite)

Constats :

- 134 115 comptes courriels non utilisés de plus de 90 jours sur un total de 305 554
- 20 240 comptes médecins ont été créés, 12 662 (pour le service courriel) ne sont pas utilisés depuis plus de 90 jours *
- 1817 comptes sont automatiquement redirigés dont 577 comptes médecins

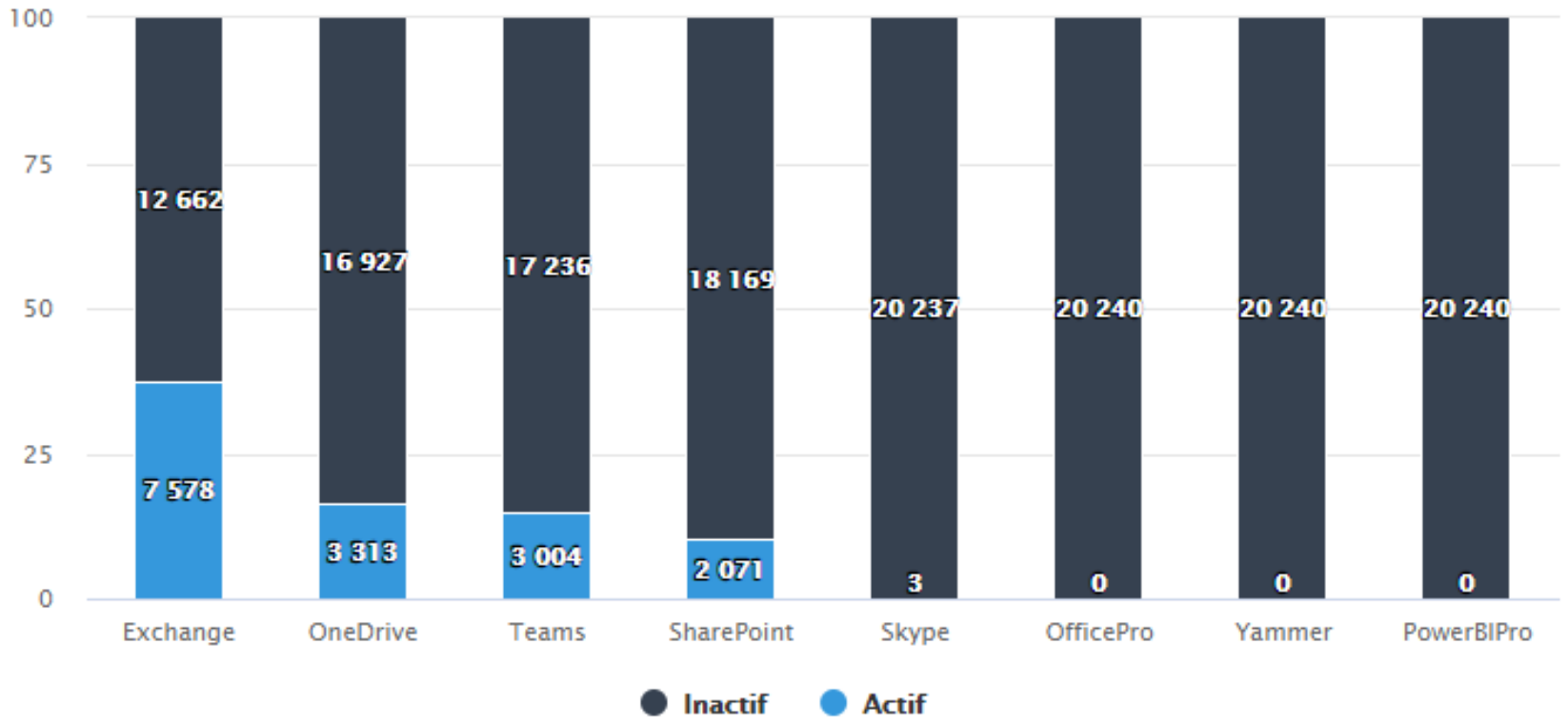
Québec

** En date du 27 octobre 2020*

5. État de situation (Suite)

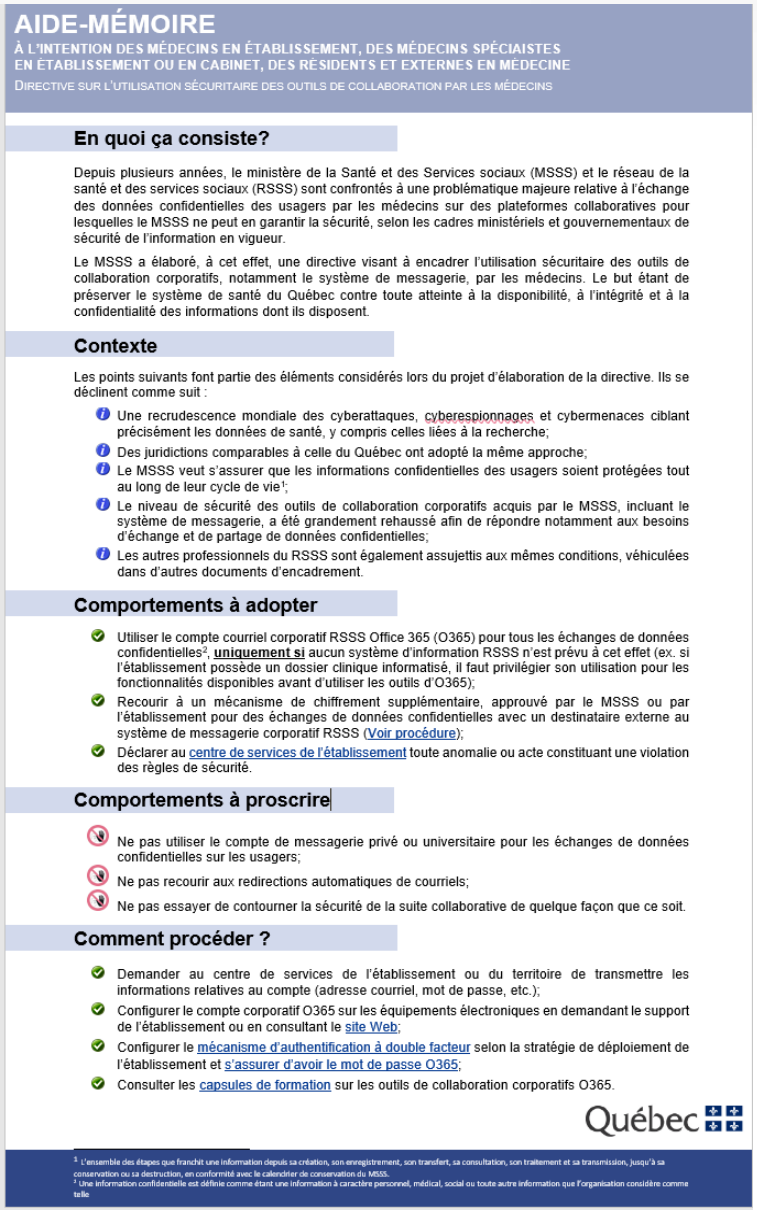
UTILISATION DU SERVICE en date du 27 octobre 2020

Exporter



Québec

6. Aide-Mémoire pour les médecins



AIDE-MÉMOIRE

À L'INTENTION DES MÉDECINS EN ÉTABLISSEMENT, DES MÉDECINS SPÉCIALISTES EN ÉTABLISSEMENT OU EN CABINET, DES RÉSIDENTS ET EXTERNES EN MÉDECINE

DIRECTIVE SUR L'UTILISATION SÉCURITAIRE DES OUTILS DE COLLABORATION PAR LES MÉDECINS

En quoi ça consiste?

Depuis plusieurs années, le ministère de la Santé et des Services sociaux (MSSS) et le réseau de la santé et des services sociaux (RSSS) sont confrontés à une problématique majeure relative à l'échange des données confidentielles des usagers par les médecins sur des plateformes collaboratives pour lesquelles le MSSS ne peut en garantir la sécurité, selon les cadres ministériels et gouvernementaux de sécurité de l'information en vigueur.

Le MSSS a élaboré, à cet effet, une directive visant à encadrer l'utilisation sécuritaire des outils de collaboration corporatifs, notamment le système de messagerie, par les médecins. 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.

Contexte

Les points suivants font partie des éléments considérés lors du projet d'élaboration de la directive. Ils se déclinent comme suit :

- Une recrudescence mondiale des cyberattaques, cyberespionnages et cybermenaces ciblant précisément les données de santé, y compris celles liées à la recherche;
- Des juridictions comparables à celle du Québec ont adopté la même approche;
- Le MSSS veut s'assurer que les informations confidentielles des usagers soient protégées tout au long de leur cycle de vie[1];
- Le niveau de sécurité des outils de collaboration corporatifs acquis par le MSSS, incluant le système de messagerie, a été grandement rehaussé afin de répondre notamment aux besoins d'échange et de partage de données confidentielles;
- Les autres professionnels du RSSS sont également assujettis aux mêmes conditions, véhiculées dans d'autres documents d'encadrement.

Comportements à adopter

- Utiliser le compte courriel corporatif RSSS Office 365 (O365) pour tous les échanges de données confidentielles[2], **uniquement si** aucun système d'information RSSS n'est prévu à cet effet (ex. si l'établissement possède un dossier clinique informatisé, il faut privilégier son utilisation pour les fonctionnalités disponibles avant d'utiliser les outils d'O365);
- Recourir à un mécanisme de chiffrement supplémentaire, approuvé par le MSSS ou par l'établissement pour des échanges de données confidentielles avec un destinataire externe au système de messagerie corporatif RSSS (Voir procédure);
- Déclarer au centre de services de l'établissement toute anomalie ou acte constituant une violation des règles de sécurité.

Comportements à proscrire

- Ne pas utiliser le compte de messagerie privé ou universitaire pour les échanges de données confidentielles sur les usagers;
- Ne pas recourir aux redirections automatiques de courriels;
- Ne pas essayer de contourner la sécurité de la suite collaborative de quelque façon que ce soit.

Comment procéder ?

- Demander au centre de services de l'établissement ou du territoire de transmettre les informations relatives au compte (adresse courriel, mot de passe, etc.);
- Configurer le compte corporatif O365 sur les équipements électroniques en demandant le support de l'établissement ou en consultant le site Web;
- Configurer le mécanisme d'authentification à double facteur selon la stratégie de déploiement de l'établissement et s'assurer d'avoir le mot de passe O365;
- Consulter les capsules de formation sur les outils de collaboration corporatifs O365.

Québec

[1] L'ensemble des étapes que franchit une information depuis sa création, 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.
[2] Une information confidentielle est définie comme étant une information à caractère personnel, médical, social ou toute autre information que l'organisation considère comme telle

Québec

7. Prochaines étapes

- Présentation au CGR
- Approbation finale et mise en vigueur

Québec

Questions, commentaires?