Guide d'accompagnement pour les services de télésanté

Chiffrer / déchiffrer un courriel

Centre intégré universitaire de santé et de services sociaux de l'Est-de-l'Île-de-Montréal
Québec

Table des matières

1. Contexte

Le chiffrement vise à sécuriser le transfert des informations entre l'expéditeur et le(s) destinataire(s) en faisant en sorte que seulement ces derniers soient en mesure de consulter le courriel.

Le présent guide vise à vous accompagner afin de mettre en place la directive du Secrétariat du Conseil du trésor qui stipule qu'un courriel doit être chiffré s'il répond **aux 2 conditions** suivantes :

1. est envoyé à un **destinataire externe** (c'est-à-dire que l'adresse n'est pas de la forme @ssss.gouv.qc.ca, ex.: @outlook.com, @gmail.com, @fournisseur_internet.com, etc.) ;

ET

2. comporte des **données confidentielles** dans le message ou dans une pièce jointe.

En bref :

Destinataire	Le courriel comporte des données confidentielles	Faut-il chiffrer le courriel ?
Interne (Courriel de la forme @ssss.gouv.qc.ca)	Oui	Non
	Non	Non
Externe (Courriel autre que @ssss.gouv.qc.ca)	Oui	**>>> Oui <<<**
	Non	Non

2. Données confidentielles

Une information confidentielle est définie comme étant une information à caractère personnel, médical, social ou toute information que l'organisation considère comme telle.

La liste non exhaustive ci-dessous présente des exemples de données confidentielles qui doivent être chiffrées si elles sont envoyées à l'externe :

1. Adresse et numéro de téléphone de l'usager ou de ses proches ;
2. Photos et vidéos où est représenté un usager (en tout ou en partie) et/ou son milieu de vie privé ;
3. Paramètres cliniques (ex.: poids, taille, signes vitaux, glycémie, etc.) ;
4. Résultats de laboratoire, de pathologie, etc. ;
5. Diagnostique.

Pour plus de détails concernant les données confidentielles, veuillez contacter le **Responsable de la sécurité de l'information** (Stéphane Gagnon, stephane_rsi.gagnon.cemtl@ssss.gouv.qc.ca) ou le service des **Archives**.

3. Revue de la trajectoire clinique

Si une trajectoire clinique de votre service de télésanté comporte l'envoi de courriels ayant des données confidentielles, vous devez :

1. Lire les Sections ci-dessous du présent document :
    - 4. Chiffrer un courriel ;
    - 5. Déchiffrer un courriel.

2. Déterminer si vous allez chiffrer seulement les courriels comportant des données confidentielles ou chiffrer tous les courriels.

    - Avantages de chiffrer tous les courriels :
        - Les intervenants n'ont pas besoin de se demander à chaque envoi s'il faut chiffrer ou non le courriel ;
        - L'usager a une expérience constante ;
        - Le fait que tous les courriels soient chiffrés peut être un élément rassurant pour l'usager, qui démontre que l'établissement porte une attention à la sécurité des communications.

    - Inconvénients de chiffrer tous les courriels :
        - L'intervenant peut parfois oublier de chiffrer le courriel ;
        - Si des intervenants de différents services communiquent avec l'usager et qu'ils n'utilisent pas tous la même méthode, l'usager pourrait être confus ;
        - L'usager pourrait trouver pénible de devoir déchiffrer tous ses courriels selon la méthode à suivre (voir Section 5.3).

    Vous devez évaluer, selon le nombre de courriels qui est envoyé et le contenu, s'il est préférable de chiffrer tous les courriels ou seulement ceux ayant des données confidentielles. Par exemple, si vous ne transmettez jamais de données confidentielles, il n'est pas pertinent de chiffrer tous les courriels.

3. Selon la décision prise au point 2, mettre votre trajectoire clinique à jour. L'équipe de la télésanté peut vous assister au besoin.

4. Diffuser la nouvelle trajectoire et donner une formation sur le chiffrement et le déchiffrement des courriels (voir Section 4 et Section 5) dans votre service.

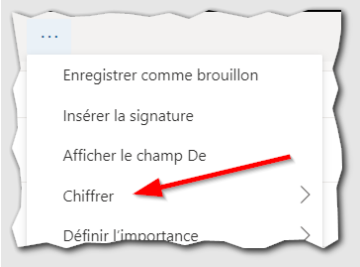
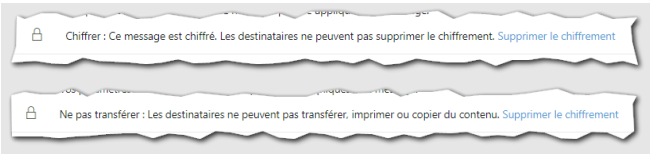
    Un accompagnement par l'équipe de télésanté est disponible. L'objectif est de former un super-utilisateur par service clinique qui agira par la suite comme premier répondant dans son service.

5. Préparer une stratégie pour informer les usagers de l'utilisation du chiffrement des courriels.
    - Nouveaux usagers :
        - Lorsqu'un nouvel usager est admis au service de télésanté, lui expliquer la procédure de déchiffrement.
    - Usagers actuels :
        - Prévoir un avis à envoyer aux usagers afin de leur indiquer que les courriels seront dorénavant chiffrés (selon l'approche qui aura été choisie : tous les courriels ou seulement ceux avec des données confidentielles).

4. Chiffrer un courriel

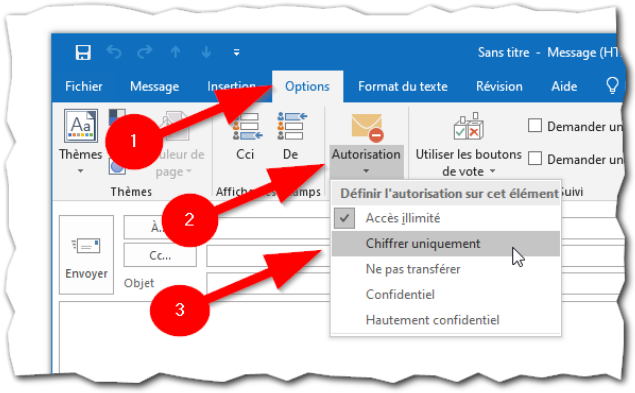
4.0 Outlook web

Pour chiffrer un courriel avec Outlook Web :

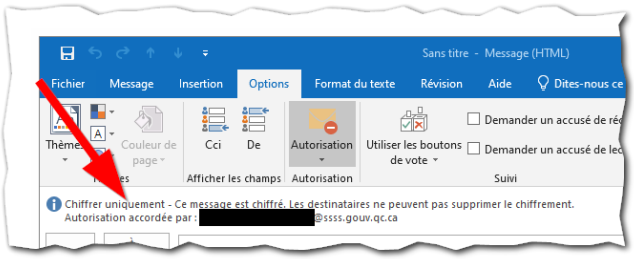
Dans un nouveau courriel, cliquez sur les points de suspension (…) à la droite du bouton **Abandonner** pour ouvrir la boîte de dialogue.	
Cliquez sur le menu **Chiffrer**.	
Cliquez sur Chiffrer dans le sous-menu **Chiffrer**.	
Une confirmation du chiffrement sera indiquée dans l'en-tête du courriel. Pour enlever le chiffrement, cliquez sur le lien **Supprimer le chiffrement**.	
Rédiger votre message comme à l'habitude et cliquer sur le bouton **Envoyer**.	

4.1 Outlook 2019

Pour chiffrer un courriel avec le client lourd d'Outlook 2019 :

Dans un nouveau message, cliquez sur le menu **Options** Cliquez sur le triangle vers le bas sous **Autorisation**. Cliquer sur le bouton **Chiffrer uniquement**.	

Un message d'information apparaît pour vous confirmer le chiffrement du message.



Rédiger votre message comme d'habitude puis cliquer sur le bouton **Envoyer**.

4.2 Outlook 2016

Si vous avez la version 2016 d'Outlook, faites une demande Octopus afin de faire installer la version 2019. Il n'y a pas de frais associés à l'installation de l'application.

Dans Octopus, allez en allant sous :

Informatique > **Logiciels & Applications** > **Installation ou configuration d'un logiciel**

5. Déchiffrer un courriel

La présente section explique la méthode pour déchiffrer un courriel qui a été chiffré.

La procédure varie selon le fournisseur du courriel :

1. Outlook, Hotmail ou autre de Microsoft ;
2. Gmail ;
3. Yahoo ;
4. Autres fournisseurs (ex.: un fournisseur d'accès internet).

Conseils

1. Il est conseillé de faire un test avec votre courriel personnel (autre que @ssss.gouv.qc.ca) afin de simuler le déchiffrement du courriel. Ceci vous permettra de vous familiariser avec le fonctionnement du déchiffrement.
2. Un guide avec la procédure de déchiffrement est disponible (lien).

   Il doit être remis en personne ou envoyé par courriel à l'usager avant de lui envoyer le premier message chiffré. Vous devez vous assurer que l'usager est à l'aise avec la procédure.

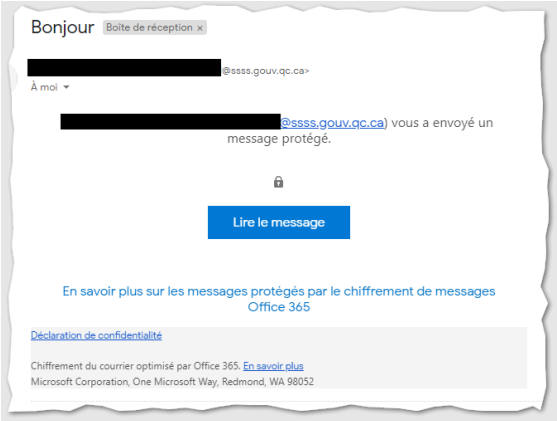
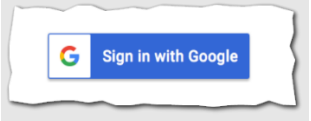
5.0 Avec un courriel Outlook, Hotmail ou autre de Microsoft

Si l'usager utilise Outlook, le courriel sera déchiffré automatiquement car il se trouve dans l'environnement sécurisé de Microsoft.

L'usager n'a rien à faire pour le lire.

5.1 Avec un courriel Gmail

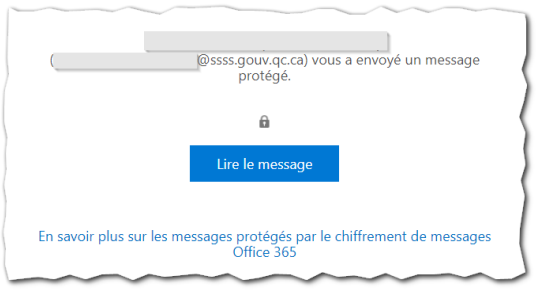
Si l'usager utilise Gmail :

L'usager recevra un courriel similaire à celui montré à droite.	
Il cliquera sur le bouton **Lire le message**.	
Une nouvelle fenêtre s'affichera. Il cliquera sur le bouton **Sign in with Google**.	
Le courriel sera alors affiché.	

5.2 Avec un courriel Yahoo

Si l'usager utilise Yahoo :

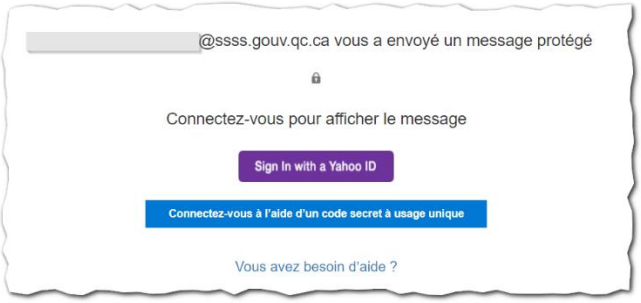
L'usager recevra un courriel similaire à celui montré à droite.



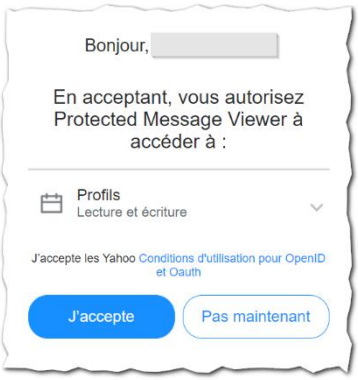
Il cliquera sur le bouton **Lire le message**.

Une nouvelle fenêtre s'affichera.

Il cliquera sur le bouton **Sing in with a Yahoo ID**.

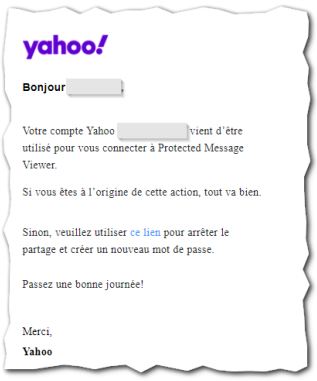


Il cliquera sur le bouton **J'accepte**.



Le courriel sera alors affiché.

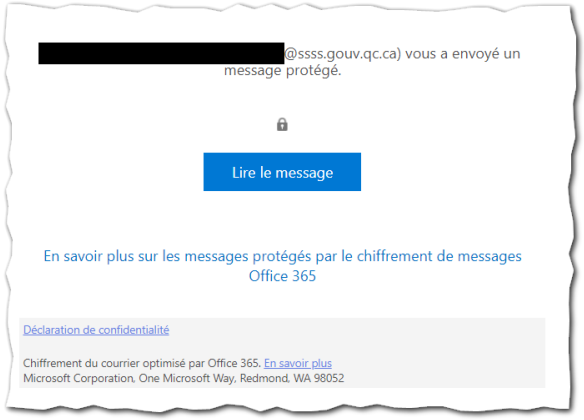
L'usager va recevoir un courriel de confirmation de Yahoo lui indiquant que son compte a été utilisé pour se connecter au courriel chiffré.



5.3 Avec tout autre courriel

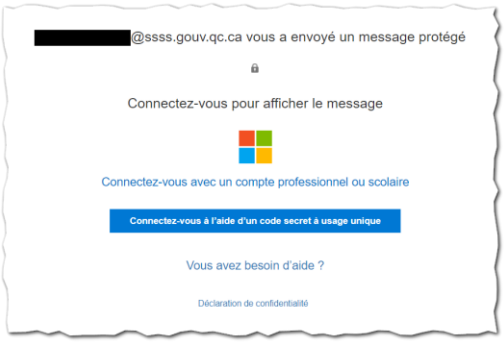
Si l'usager a un courriel autre que Outlook, Gmail, Yahoo :

L'usager recevra un courriel similaire à celui montré à droite.



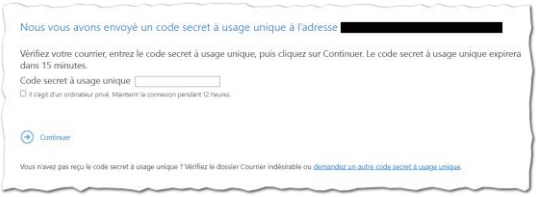
Il cliquera sur le bouton **Lire le message**.

Une nouvelle fenêtre s'affichera.

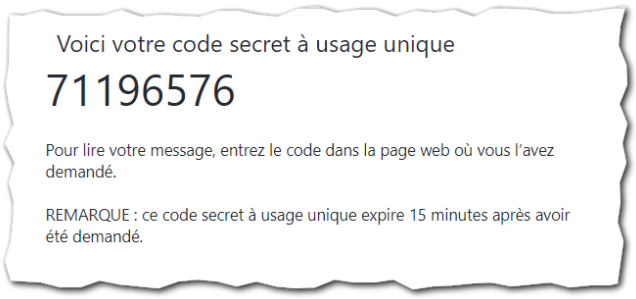
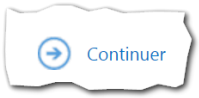


Il cliquera sur le bouton **Connectez-vous à l'aide d'un code secret à usage unique**.

Une nouvelle fenêtre s'affichera.



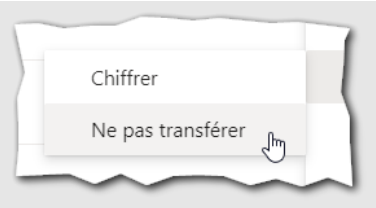
Il retournera dans sa boîte de réception de courriels.

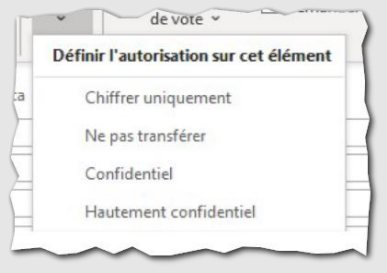
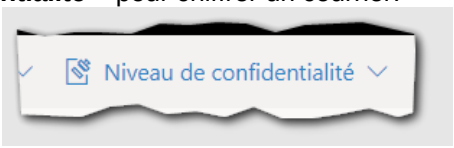
Il doit retrouvez le courriel en provenance de **Microsoft Office 365 Message Encryption**. Il doit prendre en note le numéro de 8 chiffres ou le sélectionner et faire un **Copier** (clic droit puis **Copier**).	
Il doit revenir dans la page précédente et entrer le numéro de 8 chiffres ou faire un **Coller** (clic droit puis **Coller**).	
Il doit cliquer sur **Continuer**.	
Le courriel va s'afficher.	

Note :

- Pour ce type de déchiffrement, il est préférable d'utiliser un poste de travail plutôt qu'un cellulaire ou une tablette, puisqu'il faut se déplacer entre différents écrans.
- Si vous constatez que la procédure semble complexe pour l'usager, vous pourriez lui proposer de s'ouvrir un courriel Outlook (en allant sur Outlook.com). De cette façon, le courriel sera déchiffré automatiquement.

6. Foire aux questions

Question	Réponse
Qu'est-ce qui est considéré comme une donnée confidentielle ?	Voir la Section 2. Données confidentielles.
Est-ce que je dois chiffrer tous mes courriels ?	Veuillez vous référer à votre service afin de connaître la décision qui a été prise à ce sujet.
Est-ce que je dois chiffrer un courriel comportant des données confidentielles destiné à un intervenant d'un autre établissement ayant un courriel de la forme @ssss.gouv.qc.ca ?	Non.
Est-ce que je dois chiffrer un courriel comportant des données confidentielles destiné à un intervenant d'un autre établissement qui ***n'a pas*** un courriel de la forme @ssss.gouv.qc.ca (ex. : organisme communautaire) ?	Oui.
Est-ce que je peux chiffrer un courriel à partir d'une boîte partagée ?	Oui.
Est-ce possible de chiffrer un courriel à partir de mon Outlook mobile (sur cellulaire ou tablette).	Non Il n'est pas possible de chiffrer un courriel à partir de l'application mobile d'Outlook sur un cellulaire ou une tablette. Vous devez utiliser un poste de travail.
Est-ce que je peux chiffrer un document à l'aide de l'outil de confidentialité disponible à partir d'Outlook mobile (sur cellulaire ou tablette)	Non Ne pas utiliser l'icône de la pince à papier dans le coin supérieur droit, sur la ligne de l'Objet. Il s'agit d'une autre fonctionnalité qui ne chiffre pas les courriels transmis 
Est-ce que je peux utiliser l'option « **Ne pas transférer** » ? 	Si vous utilisez l'option **« Ne pas transférer »**, le courriel sera chiffré mais l'usager ne pourra pas : • transférer le courriel à une autre personne ; • imprimer ; • copier le contenu du courriel. Vous pouvez utiliser l'option mais en étant bien conscient des impacts indiqués ci-dessus.
Dans Outlook 2019, est-il plus sécuritaire d'utiliser l'option « **Confidentiel** » ou « **Hautement confidentielle** » ?	Non. La sécurité du transfert du courriel est la même pour tous les niveaux.

Question	Réponse
	En fait, pour des destinataires à l'externe (un courriel qui n'est pas de la forme @ssss.gouv.qc.ca), vous ne devez pas utiliser « **Confidentiel** » ni « **Hautement confidentiel** » car le destinataire ne sera pas en mesure d'ouvrir le courriel.
Est-ce que je peux utiliser le bouton « **Niveau de confidentialité** » pour chiffrer un courriel? 	Non. Ce bouton fait référence à une fonctionnalité qui n'est pas disponible du côté du destinataire. Il ne sera pas en mesure d'ouvrir le courriel.
Est-ce qu'il y a moyen de faire en sorte que tous mes courriels vers l'externe soient chiffrés automatiquement ?	Non. Il n'y a malheureusement pas de configuration dans Outlook pour forcer le chiffrement.
Est-ce que je dois envoyer un mot de passe au destinataire pour qu'il puisse déchiffrer le courriel ?	Non.
Est-ce que je dois chiffrer les invitations aux téléconsultations ?	Non. En fait, il n'est pas possible de chiffrer les invitations aux téléconsultations. Ainsi, vous devez vous assurer de ne pas mettre des données confidentielles dans l'invitation.
Est-ce que l'usager doit chiffrer ses courriels pour m'envoyer des données confidentielles ?	Oui. Par contre, la plupart des fournisseurs de messagerie n'offrent pas le chiffrement dans leur forfait gratuit (ex. : Outlook, Gmail, Yahoo, etc.). Par contre, si l'usager répond à un courriel que vous avez chiffré, la réponse sera elle aussi chiffrée. Il faudrait donc demander à l'usager de ne répondre qu'à un courriel chiffré s'il doit vous transmettre des données confidentielles.
Est-ce que je peux envoyer un courriel chiffré à plusieurs personnes en même temps ou est-ce que je dois faire un courriel par personne ?	Oui. Vous pouvez faire un seul courriel, mettre tous les destinataires et chiffrer le courriel.
Est-ce que je dois chiffrer mes messages dans le clavardage d'une rencontre Teams ?	Non. La communication dans une rencontre Teams est déjà sécurisée.
J'utilisais l'application **7-Zip** auparavant pour envoyer des fichiers de manière sécurisée. Est-ce que je dois continuer ?	Non. Le chiffrement assure la sécurité du transfert du fichier vers le(s) destinataire(s).

Question	Réponse
Quelles sont les conséquences si je ne chiffre pas le courriel qui contient des données confidentielles ?	Selon la nature de l'incident, des mesures disciplinaires pourraient être appliquées par : • le CIUSSS-EMTL ; • votre ordre professionnel.

7. Support

Type de support	Contactez
Questions de compréhension sur la procédure.	La personne désignée dans votre service.
Questions sur les données confidentielles.	Contacter les Archives.
Question sur la sécurité de l'information.	Ouvrir un billet Octopus au Responsable de la sécurité de l'information (RSI) sous : **Sécurité de l'information** > **Besoin d'Information sur la sécurité de l'information** > **Information sur la sécurité d'Outlook**.
Question sur l'intégration du chiffrement dans la trajectoire du service de télésanté.	L'équipe télésanté Courriel : **telesante.cemtl@ssss.gouv.qc.ca**
Problème technique.	Ouvrir un billet **Octopus** sous : **Informatique** > **Logiciels & Applications** > **Problème avec le fonctionnement d'un logiciel auquel j'ai déjà accédé** En cas d'urgence seulement, appeler le Centre de service informatique (CSI) au **5656**.