eHealth Ontario

Guide de soutien à l'utilisation du site à l'intention des organismes utilisateurs

Services du Registre des fournisseurs

Version : 1.0

Janvier 2016

Ontario
eHealth Ontario

Avis de droit d'auteur

Tous droits réservés

Marques de commerce

Contrôle de document

La version électronique du présent document est reconnue comme étant la seule version valide.

Historique d'approbation

APPROBATEUR(S)	TITRE/SERVICE	DATE D'APPROBATION
Samara Strub	Analyste de la protection de la vie privée, protection de la vie privée	2015-11-17
Suchun Wu	Conseiller principal en sécurité des TI, sécurité	2015-11-17
Michael Conde	Chef, registres provinciaux	2016-01-07
Cynthia Zhang	Chef des relations, identité, accès et protection de la vie privée	2016-01-07

Historique de révision

N° DE VERSION	DATE	RÉSUMÉ DES MODIFICATIONS	MODIFIÉ PAR
1.0	2016-01-11	Publication de la version initiale	Identité, accès et protection de la vie privée

Niveau de sensibilité du document

Moyen

Table des matières

À propos du présent document

Contexte

Destiné à toutes les solutions de dossiers de santé électroniques (DSE), le Registre des fournisseurs (RF) constitue la source de renseignements faisant autorité au sujet des professions de la santé et des lieux de prestation de soins de santé. Le RF facilite l'identification unique et exacte des personnes et des organismes réglementés qui fournissent des services de santé en Ontario ou qui participent à la collecte, à l'utilisation ou à la divulgation de renseignements personnels sur la santé (RPS) dans l'ensemble du continuum de soins. Le RF contient des renseignements fiables au sujet des professionnels et des organismes de santé réglementés en Ontario qui sont visés par la définition de dépositaire de renseignements sur la santé (DRS) ou d'exploitant d'un DRS en vertu de la *Loi de 2004 sur la protection des renseignements personnels sur la santé* (LPRPS). Le RF est alimenté par les ordres de réglementation, les bases de données du ministère de la Santé et des Soins de longue durée, les hôpitaux et d'autres organismes, et est géré par cyberSanté Ontario.

Il vise à :

- établir clairement l'identité des fournisseurs réglementés;
- fournir des renseignements sur les fournisseurs (p. ex., statut du permis, lieux de pratique).

Exemples de services fournis par le RF :

- recherche et détermination de l'identité d'un fournisseur particulier;
- recherche et détermination des données et des emplacements d'un organisme fournisseur.

Objet et portée du document

Le présent document a pour objet de fournir aux organismes utilisateurs du RF des renseignements et des lignes directrices en matière de soutien à l'utilisation du site suivant l'entrée en service. Le présent document définit clairement ce qu'il faut faire pour obtenir du soutien de cyberSanté Ontario relativement à tout problème lié au RF et aide les nouveaux utilisateurs dans le cadre de la transition opérationnelle.

Public cible

Ce document s'adresse à toutes les personnes qui interagiront avec le RF au sein des organismes utilisateurs.

1 Introduction

Le Guide de soutien à l'utilisation du site à l'intention des organismes utilisateurs des services du Registre des fournisseurs est un document complet présentant les différents processus élaborés en vue d'aider les organismes utilisateurs au moment de connecter de nouveaux établissements au RF. Il fournit des renseignements relatifs au soutien et à la maintenance, ainsi que des procédures et des obligations en matière de sécurité.

1.1 Soutien

Le Service de dépannage de cyberSanté Ontario constitue le principal mécanisme de soutien pour tous les utilisateurs des services de cyberSanté Ontario. On décrit ci-dessous la façon de solliciter l'aide du Service de dépannage et les processus connexes.

1.1.1 Communiquer avec le Service de dépannage pour obtenir du soutien

Le Service de dépannage de cyberSanté Ontario représente le point de contact unique pour les demandes de service concernant les problèmes liés au RF. Au Service de dépannage de cyberSanté Ontario, des agents sont disponibles 24 heures par jour, 7 jours par semaine pour répondre aux demandes.

Comment joindre le Service de dépannage de cyberSanté Ontario

Le Service de dépannage est ouvert 7 jours par semaine, 24 heures par jour.

Numéro local : 905 826-5551
Sans frais : 1 866 250-1554
Option 1 – Soutien technique (utilisateurs existants)
Option 2 – Soutien à l'inscription (nouveaux utilisateurs)
Courriel : servicedesk@ehealthontario.on.ca

Pour d'autres coordonnées de cyberSanté Ontario, consultez le site :
http://www.ehealthontario.on.ca/fr/contact/.

1.1.2 Créer une demande de service

Par téléphone – Méthode suggérée pour les problèmes et incidents de gravité élevée (p. ex., la production est en panne ou l'environnement est grandement détérioré)

Par courriel – Méthode suggérée pour les problèmes de gravité moyenne ou faible

1.1.3 Liste de vérification pour favoriser un service rapide

✓	Activité
☐	Nom
☐	Emplacement de l'établissement
☐	Coordonnées de la personne-ressource (et de personnes-ressources secondaires, le cas échéant)
☐	Service de cyberSanté Ontario
☐	Environnement du service de cyberSanté Ontario touché (p. ex., production ou essais de conformité)
☐	Description du problème (inclure la date et l'heure auxquelles le problème s'est produit et le nombre d'utilisateurs touchés, s'il est connu)
☐	Mesures prises pour reproduire le problème et en déterminer la cause

1.1.4 Demande de service et renvoi à l'échelon supérieur

Nº	Étape	Description
1	Demande de service	• L'organisme utilisateur communique avec cyberSanté Ontario pour effectuer une demande de service. • L'organisme utilisateur sélectionne l'option du Service de dépannage dans le menu téléphonique.
2	Entretien avec l'équipe de première ligne du Service de dépannage	• L'agent du Service de dépannage de cyberSanté Ontario travaille avec l'organisme utilisateur pour déterminer le ou les problème(s) et entreprendre les étapes de dépannage. • L'agent du Service de dépannage de cyberSanté Ontario peut s'adresser à un responsable technique de cyberSanté Ontario au besoin. • L'agent du Service de dépannage peut demander des renseignements supplémentaires à l'organisme utilisateur pour orienter le processus de dépannage. • Une fois toutes les mesures prises, si l'agent du Service de dépannage n'a pas réussi à régler le problème et que la résolution de ce dernier n'a pas progressé, le problème peut être renvoyé à l'équipe de soutien du niveau suivant de cyberSanté Ontario.
3	Renvoi du problème à l'équipe de soutien du niveau suivant de cyberSanté Ontario	• Le problème est assigné au niveau de soutien suivant. • Le niveau de soutien suivant désigné communique avec l'organisme utilisateur. • Le niveau de soutien suivant examine le problème et poursuit les activités de dépannage selon les besoins. • S'il y a lieu, d'autres équipes de soutien sont mises à contribution pour poursuivre les efforts de résolution du problème.

1.1.5 Résolution de la demande de service

Mises à jour – Pour connaître l'évolution d'une demande de service, veuillez communiquer avec le Service de dépannage. Par ailleurs, des mises à jour automatisées sont envoyées lorsque la demande de service est renvoyée à une autre équipe.

Priorité de la demande de service – La priorité d'un incident est établie par l'agent de soutien et l'organisme utilisateur de façon mutuelle.

Clôture de la demande de service – Une demande de service sera close 15 jours après la résolution du problème, s'il est impossible d'offrir une assistance plus avancée ou si l'organisme utilisateur autorise l'équipe de soutien de cyberSanté Ontario à clore la demande. En outre, une demande sera fermée s'il est impossible de joindre l'organisme utilisateur après trois tentatives de communication. Le cas échéant, l'organisme utilisateur recevra trois rappels, dont un rappel final indiquant que la demande sera fermée le jour suivant.

1.1.6 Satisfaction des utilisateurs

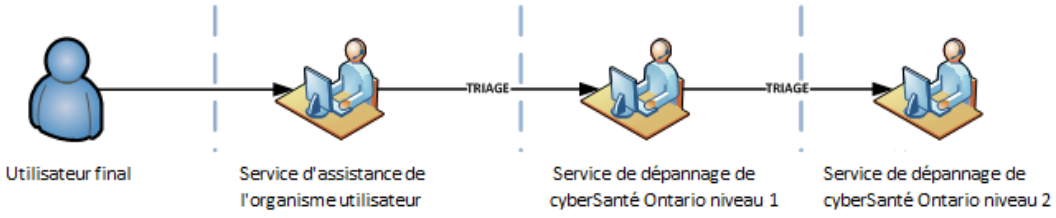
Le Service de dépannage de cyberSanté Ontario a à cœur la satisfaction des organismes utilisateurs. Nous sommes ouverts aux commentaires et encourageons les utilisateurs à participer en ayant recours à l'un des moyens suivants :

Sondage sur la satisfaction des utilisateurs
Lors de la fermeture des demandes de service, cyberSanté Ontario sélectionne au hasard des incidents qui feront l'objet d'un sondage. Il est donc possible que des utilisateurs soient invités à répondre à un questionnaire en ligne. Nous sommes reconnaissants envers les utilisateurs qui nous aident à assurer la qualité de notre service en répondant à un bref sondage d'une durée de cinq minutes.

Commentaires généraux
Veuillez écrire à l'adresse servicedesk@ehealthontario.on.ca pour formuler des commentaires ou des suggestions.

1.2 Processus de soutien

1.1.7 Représentation générale du modèle de soutien du RF



1.1.8 Responsabilités du service d'assistance de l'organisme utilisateur

Lorsqu'un problème lié à l'interface utilisée pour accéder aux données du RF est détecté, le service d'assistance de l'organisme utilisateur de chaque établissement offre du soutien aux utilisateurs de l'établissement afin de :

- découvrir la cause du problème;
- proposer une résolution dans la mesure du possible;
- déterminer l'incidence potentielle des problèmes;
- renvoyer la demande aux groupes de soutien appropriés et (ou) au Service de dépannage de cyberSanté Ontario.

1.1.9 Quand un organisme utilisateur doit-il communiquer avec le Service de dépannage de cyberSanté Ontario?

Communiquez avec le Service de dépannage de cyberSanté Ontario lorsque vous avez des renseignements ou des questions, notamment pour :

- demander de l'aide afin de régler des problèmes liés à l'interface du RF;
- signaler une erreur de l'application du RF (consultez Annexe – Tableau des codes d'erreur du RF);
- signaler une infraction à la politique sur la protection de la vie privée.

Vous pouvez aussi joindre le Service de dépannage pour obtenir des renseignements de cyberSanté Ontario au sujet de ce qui suit :

- fonctionnalités du RF;
- protection de la vie privée et sécurité des renseignements personnels du RF.

Remarque : Les utilisateurs finaux devraient toujours communiquer avec le service d'assistance de leur établissement pour obtenir de l'aide relativement aux problèmes liés au RF. Le service d'assistance de l'établissement jugera si le problème doit être transmis au Service de dépannage de cyberSanté Ontario. Les utilisateurs finaux **ne devraient pas** communiquer avec le Service de dépannage de cyberSanté Ontario sans avoir d'abord consulté le service d'assistance de leur établissement.

1.1.10 Quand le Service de dépannage de cyberSanté Ontario communique-t-il avec l'organisme utilisateur?

- pour obtenir des précisions au sujet d'un incident que vous avez signalé ou d'une demande de service que vous avez effectuée;
- pour vous informer des activités de maintenance pouvant avoir des répercussions sur le service;
- pour signaler une interruption de l'interface du RF;
- pour fournir de l'information concernant nos activités d'amélioration des applications et les dates de publication des nouvelles versions.

1.1.11 Quand le Bureau de la protection de la vie privée de cyberSanté Ontario communique-t-il avec l'organisme utilisateur?

- pour obtenir des renseignements supplémentaires afin de répondre aux demandes d'accès au RF;
- aux fins de gestion des incidents.

2 Responsabilités opérationnelles relatives aux données du RF

2.1 Registres de vérification

En vertu des ententes que nous avons avec les ordres de réglementation pertinents qui fournissent des données au RF de cyberSanté Ontario, ainsi que des ententes conclues avec les organismes utilisateurs participants, il incombe à cyberSanté Ontario de tenir un dossier électronique de tous les accès aux données du RF dans un système de cyberSanté Ontario. En raison de cette exigence, cyberSanté Ontario doit avoir accès à une copie des registres de vérification de l'organisme utilisateur. On pourrait demander à cyberSanté Ontario de fournir un rapport de vérification de ces registres.

2.2 Conservation et élimination des données du RF

Les données recueillies auprès du RF aux fins d'utilisation à l'établissement de l'organisme utilisateur ne devraient être conservées que pendant la période où l'établissement en a besoin aux fins autorisées prévues par les ententes pertinentes. Après cette période, les données du RF devraient être éliminées de façon sécuritaire.

3 Protection de la vie privée et sécurité

3.1 Questions relatives aux données

Si un organisme utilisateur reçoit des plaintes ou des questions de la part d'usagers ou de fournisseurs relativement aux données du RF, l'établissement doit signaler la question ou la plainte au Service de dépannage de cyberSanté Ontario dès que cela est raisonnablement possible après l'avoir reçue, et collaborer avec cyberSanté Ontario afin d'examiner les plaintes mettant en cause les données du RF et y répondre.

3.2 Questions relatives aux processus

Si un organisme utilisateur reçoit des plaintes ou des questions de la part d'usagers ou de fournisseurs concernant cyberSanté en général (p. ex., sans lien avec les données du RF), ou concernant les politiques et les méthodes en matière de protection de la vie privée de cyberSanté Ontario (y compris la manière dont il faut répondre aux demandes d'accès individuelles, et les processus de gestion des incidents ou des infractions), l'établissement doit indiquer à la personne ayant formulé la plainte ou la question de soumettre sa plainte, ses préoccupations ou sa question par téléphone, par courriel, par télécopieur ou par la poste au directeur de la protection des renseignements personnels :

Bureau de la protection de la vie privée de cyberSanté Ontario
Case postale 148
777, rue Bay, bureau 701
Toronto (Ontario) M5G 2C8
Tél. : 416 946-4767
Téléc. : 416 586-6598
Courriel : privacy@ehealthontario.on.ca

> **Remarque :** *Lorsque vous envoyez des courriels à cyberSanté Ontario, il est extrêmement important de ne divulguer aucun renseignement personnel sur les patients et sur leur santé.*

3.3 Gestion des incidents et des infractions

Un processus de gestion des incidents et des infractions liés à la protection de la vie privée et à la sécurité a été créé pour prendre en charge les incidents ou les infractions, réels ou présumés, liés à la sécurité ou à la protection de la vie privée signalés à cyberSanté Ontario. Le processus de signalement d'un incident ou d'une infraction lié à la sécurité ou à la protection de la vie privée est décrit ci-dessous et prend en charge les scénarios suivants :

i) incidents ou infractions relevés par les personnes-ressources du Service de dépannage d'un organisme utilisateur;
ii) incidents ou infractions relevés par les usagers des organismes utilisateurs;
iii) incidents ou infractions relevés par cyberSanté Ontario et qui ont des répercussions sur les organismes utilisateurs.

Définition d'un incident lié à la protection de la vie privée :

- Une contravention aux politiques, méthodes ou pratiques en matière de protection de la vie privée mises en place par un organisme utilisateur et cyberSanté Ontario, qui n'entraîne pas la cueillette, l'utilisation, la divulgation ou la destruction non autorisée des renseignements personnels, ou qui ne contrevient pas aux lois applicables en matière de protection de la vie privée.
- Une contravention, de la part d'un organisme utilisateur, à tout accord conclu avec cyberSanté Ontario qui ne contrevient pas aux lois applicables en matière de protection de la vie privée.
- Une contravention à tout accord conclu entre cyberSanté Ontario et un organisme utilisateur accédant au RF au moyen de l'interface de ce site, qui ne contrevient pas aux lois applicables en matière de protection de la vie privée.
- Une infraction présumée liée à la protection de la vie privée.

Définition d'une infraction liée à la protection de la vie privée :

- La cueillette, l'utilisation et la divulgation de renseignements personnels contrevenant à la LAIPVP et à ses règlements.
- Situations où des renseignements personnels sont volés, perdus ou recueillis, utilisés, divulgués, copiés, modifiés, conservés ou éliminés de façon non autorisée ou inappropriée.

Définition d'un incident lié à la sécurité :

- Une violation ou une menace imminente de violation des politiques relatives à la sécurité informatique, des politiques sur l'utilisation acceptable ou des pratiques de sécurité standard.

- Ces violations sont classées comme suit : programme, exploration et balayage malveillants, déni de service, accès non autorisé et utilisation inappropriée.

Les organismes utilisateurs et cyberSanté Ontario doivent former les employés, les agents et les fournisseurs de services participant au processus de gestion des incidents énoncé ci-dessous afin qu'ils connaissent leurs rôles et leurs responsabilités à l'égard de ce dernier.

Les organismes utilisateurs doivent également transmettre à leurs usagers la procédure appropriée pour signaler les incidents ou les infractions, réels ou présumés, liés à la protection de la vie privée impliquant les données du RF auxquelles cet établissement a eu accès, conformément aux étapes indiquées dans le présent document.

Incidents ou infractions liés à la sécurité ou à la protection de la vie privée relevés par un organisme utilisateur ou ses usagers :

1. Lorsque des usagers relèvent un incident ou une infraction lié à la sécurité ou à la protection de la vie privée, ceux-ci doivent communiquer immédiatement avec leur Service de dépannage local et (ou) avec le responsable interne de la protection de la vie privée et de la sécurité.
2. La ou les personnes-ressources désignées de l'organisme utilisateur (personne-ressource autorisée de l'établissement, personne-ressource du Service de dépannage et [ou] responsable de la protection de la vie privée et de la sécurité de l'établissement), collectivement appelées la « personne-ressource », communique avec le Service de dépannage de cyberSanté Ontario par téléphone au 1 866 250-1554, dès qu'elle a pris connaissance d'un incident ou d'une infraction, réel ou présumé, lié à la sécurité ou à la protection de la vie privée, impliquant ou pouvant impliquer les données du RF; le Service de dépannage ou l'agent de la protection de la vie privée de l'organisme utilisateur, en collaboration avec cyberSanté Ontario, est chargé de maîtriser de tels incidents liés à la protection de la vie privée et à la sécurité, et de consigner toutes les mesures entreprises pour maîtriser la situation et (ou) y remédier. Cette documentation ne doit contenir aucun renseignement personnel ou RPS.
3. Pour un incident ou une infraction lié à la sécurité ou à la protection de la vie privée impliquant le RF, la personne-ressource ne doit pas communiquer directement avec les fournisseurs, les patients ou les mandataires spéciaux, à moins d'en avoir reçu l'ordre par écrit de la part de cyberSanté Ontario.
4. Le Service de dépannage ouvrira un formulaire d'intervention en cas d'incident relatif à la sécurité ou un formulaire de gestion des infractions à la politique de protection de la vie privée, et l'attribuera à l'équipe correspondante.
5. L'équipe d'intervention en cas d'incident relatif à la sécurité ou de gestion des infractions à la politique de protection de la vie privée de cyberSanté Ontario communiquera avec la personne-ressource afin de recevoir une mise à jour sur l'enquête menée par l'établissement.
6. Si nécessaire, le responsable de l'équipe d'intervention en cas d'incident relatif à la sécurité ou de gestion des infractions à la politique de protection de la vie privée demandera à l'établissement une copie de toute information connexe qui pourrait s'avérer utile pour cyberSanté Ontario dans le cadre de ses propres activités de gestion de l'incident. Les registres et (ou) autres renseignements de nature délicate doivent être transmis à cyberSanté Ontario par courriel, sous forme de document chiffré.
7. L'organisme utilisateur doit accomplir toutes les mesures visant à remédier à la situation, selon les directives de cyberSanté Ontario, et mettre en œuvre des mesures préventives pour éviter que l'incident ne se reproduise et pour assurer la confidentialité et la sécurité des données du RF.

8. On peut demander à la personne-ressource de fournir à cyberSanté Ontario un exemplaire du rapport d'incident à la clôture de l'incident ou de l'infraction lié à la sécurité ou à la protection de la vie privée.
9. La personne-ressource doit détruire les documents relatifs à l'enquête sur l'incident une fois que le rapport d'incident a été envoyé à cyberSanté Ontario et que ce dernier lui a indiqué que l'incident ou l'infraction, réel ou présumé, est clos.

Incidents ou infractions liés à la sécurité ou à la protection de la vie privée relevés par un organisme utilisateur et signalés directement à cyberSanté Ontario :

1. Les usagers des organismes utilisateurs communiquent directement avec cyberSanté Ontario pour signaler un incident ou une infraction, réel ou présumé, lié à la sécurité ou à la protection de la vie privée.
2. Le Service de dépannage ouvrira un formulaire d'intervention en cas d'incident relatif à la sécurité ou un formulaire de gestion des infractions à la politique de protection de la vie privée et l'attribuera à l'équipe correspondante.
3. Le responsable de l'équipe d'intervention en cas d'incident relatif à la sécurité ou de gestion des infractions à la politique de protection de la vie privée communiquera avec la personne-ressource pour l'aviser de l'incident ou de l'infraction, réel ou présumé, lié à la sécurité ou à la protection de la vie privée.
4. La personne-ressource aidera le responsable de l'équipe d'intervention en cas d'incident relatif à la sécurité ou de gestion des infractions à la politique de protection de la vie privée à mener une enquête sur l'incident ou l'infraction, réel ou présumé, lié à la sécurité ou à la protection de la vie privée, et à maîtriser la situation.
5. Au besoin, le responsable de l'équipe d'intervention en cas d'incident relatif à la sécurité ou de gestion des infractions à la politique de protection de la vie privée demandera à l'établissement une copie de toute information requise qui pourrait s'avérer utile pour l'enquête ou les communications.
6. Les registres et (ou) autres renseignements de nature délicate doivent être transmis à cyberSanté Ontario par courriel, sous forme de document chiffré.
7. La personne-ressource doit accomplir toutes les mesures visant à remédier à la situation, selon les directives de cyberSanté Ontario, afin d'éviter que l'incident ne se reproduise et d'assurer la confidentialité et la sécurité des données du RF. On peut demander à l'établissement de fournir à cyberSanté Ontario un exemplaire du rapport d'incident à la clôture de l'incident ou de l'infraction lié à la sécurité ou à la protection de la vie privée.
8. La personne-ressource doit détruire les documents relatifs à l'enquête sur l'incident une fois que le rapport d'incident a été envoyé à cyberSanté Ontario et que ce dernier lui a indiqué que l'incident ou l'infraction, réel ou présumé, est clos.

Incident ou infraction lié à la sécurité ou à la protection de la vie privée relevé par cyberSanté Ontario :

1. Un incident ou infraction lié à la sécurité ou à la protection de la vie privée est relevé par cyberSanté Ontario.
2. Le Service de dépannage est avisé de l'incident.
3. Le Service de dépannage ouvre un formulaire d'intervention en cas d'incident relatif à la sécurité ou un formulaire de gestion des infractions à la politique de protection de la vie privée, et l'attribue à l'équipe correspondante.
4. L'équipe d'intervention en cas d'incident relatif à la sécurité ou de gestion des infractions à la politique de protection de la vie privée procède à une enquête sur l'incident. Si, durant l'enquête, on

établit que l'incident lié à la sécurité ou à la protection de la vie privée a une incidence sur un organisme utilisateur, les responsables de la protection de la vie privée ou de la sécurité en avisent la personne-ressource attitrée à l'incident.

5. La personne-ressource aide les responsables de la protection de la vie privée ou de la sécurité à maîtriser la situation, à mener une enquête sur l'incident et à résoudre l'incident.

La personne-ressource doit accomplir toutes les mesures visant à remédier à la situation, selon les directives de cyberSanté Ontario, afin d'éviter que l'incident ne se reproduise.

Renseignements qui doivent être fournis au Service de dépannage de cyberSanté Ontario lorsqu'on signale une infraction liée à la protection de la vie privée et à la sécurité :

Lorsqu'elle signale un incident ou une infraction lié à la protection de la vie privée et à la sécurité à cyberSanté Ontario, la personne-ressource doit fournir les renseignements suivants :

1. Description de la situation et conditions ayant mené à l'incident.
2. Qui appelle et qui est impliqué (noms et rôles)?
3. Où s'est produit l'incident?
4. Quand et à quelle heure l'incident a-t-il été relevé?
5. Décrire de quelle manière l'incident a été relevé.
6. Si possible, fournir des renseignements sur la situation et les conditions qui ont mené à l'incident. Par exemple :
    - Erreur humaine
    - Négligence
    - Défaillance technique causée par l'incapacité d'une application ou d'un système à préserver la confidentialité
    - Défaillance du processus causée par le non-respect du processus
    - Transgression intentionnelle
    - Acte de la nature
7. Quels renseignements sont impliqués et sous quel format (c.-à-d. support papier ou électronique)?
8. Quels systèmes sont impliqués?
9. Si possible, dresser la liste des mesures entreprises pour protéger les renseignements personnels/RPS à la suite de l'incident.
10. Si possible, dresser la liste de toutes les mesures correctives mises en œuvre ou de toutes les mesures de contrôle mises de l'avant.

Remarque : *Lorsque vous signalez une infraction ou un incident réel ou soupçonné à un agent du Service de dépannage de cyberSanté Ontario, il est extrêmement important de ne divulguer aucun renseignement personnel sur les patients et sur leur santé.*

4 Annexe

4.1 Codes d'erreur du RF

	Code	Nom d'affichage	Description
1.	NS200	Interaction non prise en charge	L'interaction (ou : cette version de l'interaction) n'est pas prise en charge.
2.	NS202	Identifiant de traitement non pris en charge	L'identifiant de traitement n'est pas pris en charge.
3.	NS203	Identifiant de version non pris en charge	L'identifiant de version n'est pas pris en charge.
4.	NS250	Mode de traitement non pris en charge	Le mode de traitement n'est pas pris en charge.
5.	NS260	Expéditeur inconnu	L'identifiant du dispositif de l'expéditeur est inconnu.
6.	INTERR	Erreur interne du système	Un composant interne du logiciel a présenté une défaillance (base de données, application, mécanisme de file d'attente, etc.), et le message n'a donc pas pu être traité.
7.	NOSTORE	Aucun espace pour stocker le message.	Rejet : Le message ne peut pas être stocké par le destinataire en raison d'un problème interne non spécifié lié à l'application. Le message n'a pas été traité ni stocké par l'application de destination.
8.	RTEDEST	Erreur d'acheminement du message, destination inaccessible.	Erreur : La destination de ce message est connue de l'application de destination. Des messages ont déjà été acheminés avec succès à cette destination. Le lien menant à l'application de destination ou à une application de rechange n'est pas disponible.
9.	RTUDEST	Erreur : erreur d'acheminement du message, destination inconnue.	La destination de ce message est inconnue de l'application de destination. L'application de destination ne correspond pas à l'application qui a reçu le message. Le message n'a pas été acheminé, traité ou stocké par l'application de destination.
10.	RTWDEST	Avertissement concernant l'acheminement du message, destination inaccessible.	Avertissement : La destination de ce message est connue de l'application de destination. Des messages ont déjà été acheminés avec succès à cette destination. Le lien menant à l'application de destination ou à une application de rechange est (temporairement) indisponible. L'application de destination transférera le message dès qu'il sera à nouveau possible de joindre la destination.
11.	SYN	Erreur de syntaxe	Indique les erreurs concernant la syntaxe ou la structure de la communication.
12.	NS200	Interaction non prise en charge	L'interaction (ou : cette version de l'interaction) n'est pas prise en charge.