cyberSanté Ontario
Travaille pour vous

Politique de confidentialité

Dossier de santé électronique

Ontario
cyberSanté Ontario

Table des matières

eHealth Ontario

Politique sur l'accès aux renseignements et la rectification des renseignements

Dossier de santé électronique

Version : 2.0

N° de document : 3871

Ontario
eHealth Ontario

Gestion du document

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

Historique des approbations

APPROBATEURS	DATE D'APPROBATION
Membres du comité de protection de la vie privée ConnectingPrivacy	17 mars 2016

Historique des révisions

NUMÉRO DE VERSION	DATE AAAA-MM-JJ	RÉSUMÉ DES CHANGEMENTS	AUTEUR DES CHANGEMENTS
2.0	2016-12-01	Révisions conformément à l'évaluation des politiques par le CPC	Rand Muhtam, analyste en protection de la vie privée, cyberSanté Ontario
1.1	2015-11-25	Révisions mineures – mise à jour pour ConnexionOntario	Samara Strub, analyste en protection de la vie privée, cyberSanté Ontario
1.0	2014-11-17	Version définitive	Urooj Kirmani, analyste principal en protection de la vie privée, cyberSanté Ontario
0.01	2014-11-04	Première version établie en fonction de la politique harmonisée sur l'accès aux renseignements et la rectification des renseignements du comité de protection de la vie privée ConnectingPrivacy, v1.1	Promila Gonsalves, analyste en protection de la vie privée, cyberSanté Ontario

Table des matières

1 Objectif

Définir les politiques, les procédures et les pratiques qui s'appliquent à la réception de demandes d'accès et de demandes de rectification concernant les dossiers de renseignements personnels sur la santé (RPS) dans le dossier de santé électronique (DSE) faites par la personne[1] que concernent les RPS ainsi qu'à la réponse à ces demandes.

2 Portée

La présente politique et les procédures connexes s'appliquent aux demandes d'accès et aux demandes de rectification concernant les dossiers de RPS dans le DSE.

La présente politique et les procédures connexes ne s'appliquent pas aux demandes d'accès et aux demandes de rectification concernant les dossiers de RPS qui n'ont pas été versés dans le DSE. Le DSE est composé de la solution ConnexionOntario et du Dépôt des Services communs d'imagerie diagnostique. La solution ConnexionOntario et le Dépôt des Services communs d'imagerie diagnostique sont des dépôts ou des systèmes auxiliaires cliniques destinés à stocker et à rendre accessibles des renseignements personnels sur la santé contenus dans les systèmes électroniques de renseignements sur la santé des dépositaires de ces renseignements[2].

3 Politique

3.1 Fondements

3.1.1 La *Loi de 2004 sur la protection des renseignements personnels sur la santé* (LPRPS) autorise une personne à formuler une demande d'accès aux dossiers contenant ses RPS sous la garde ou le contrôle d'un dépositaire de renseignements sur la santé (DRS) et une demande de rectification de ces renseignements et oblige les DRS à donner suite à la demande sous réserve d'exceptions limitées et précises.

3.1.2 Conformément à la LPRPS, les DRS doivent répondre à une demande d'accès et à une demande de rectification dans les trente (30) jours suivant la réception de la demande ou peuvent, dans les trente (30) jours suivant la réception de la demande, prolonger le délai pour une période supplémentaire de trente (30) jours en vertu de la Partie V de la LPRPS et après en avoir avisé la personne par écrit.

3.1.3 La LPRPS permet aux DRS d'exiger des frais pour donner l'accès à un dossier de RPS ou fournir une copie du dossier de RPS à la personne si cette dernière obtient d'abord une estimation des frais et si le montant des frais ne dépasse pas le montant raisonnable permettant de récupérer les coûts de l'accès.

3.1.4 Les DRS et cyberSanté Ontario doivent avoir en place les politiques, les procédures et les pratiques sur la protection de la vie privée et la sécurité nécessaires pour les rendre conformes à leurs obligations aux termes de la LPRPS, des ententes applicables ainsi que de la présente politique et des procédures connexes.

3.1.5 Les DRS et cyberSanté Ontario doivent avoir en place des politiques, des procédures et des pratiques sur la protection de la vie privée et la sécurité qui respectent la LPRPS et informer leurs mandataires et leurs fournisseurs de services électroniques sur les politiques, les procédures et les pratiques imposées par la LPRPS.

3.1.6 cyberSanté Ontario doit avoir un programme leur permettant, à lui et aux DRS, de remplir leurs obligations par rapport à la réception de demandes d'accès et de demandes de rectification concernant des dossiers de RPS dans le

[1] Le terme *personne* inclut aussi le mandataire spécial de la personne le cas échéant.

[2] Les divergences entre les exigences des politiques et des procédures de la solution ConnexionOntario et du Dépôt des Services communs d'imagerie diagnostique sont indiquées dans la présente politique.

DSE et la réponse à ces demandes conformément à la LPRPS, aux ententes applicables ainsi qu'à la présente politique et aux procédures connexes.

3.1.7 Les DRS et cyberSanté Ontario doivent prendre les mesures nécessaires et raisonnables selon les circonstances afin que leurs mandataires et leurs fournisseurs de services électroniques se conforment à la LPRPS, aux ententes applicables ainsi qu'à la présente politique et aux procédures connexes.

3.1.8 La présente politique et les procédures connexes permettent à une personne d'exercer le droit que lui accorde la loi de faire une demande d'accès et une demande de rectification concernant ses dossiers de RPS dans le DSE et aident les DRS à respecter les obligations que leur impose la LPRPS quant à la réception des demandes d'accès et des demandes de rectification et à la réponse à ces demandes.

3.1.9 Sans limiter la portée du paragraphe 3.1.1, les personnes auront le droit de faire une demande d'accès aux dossiers suivants de RPS dans le DSE :

- les dossiers cliniques de la personne;
- les dossiers relatifs à tous les cas où la totalité ou une partie des RPS de la personne est consultée, manipulée ou autrement employée par les DRS ou leurs mandataires et leurs fournisseurs de services électroniques;
- les dossiers relatifs à tous les cas où une directive sur le consentement est formulée, modifiée ou retirée par la personne;
- les dossiers relatifs à tous les cas où on déroge à une directive sur le consentement formulée par la personne et la raison de la dérogation.

3.1.10 Les hôpitaux soumis à la *Loi sur l'accès à l'information et la protection de la vie privée* (LAIPVP) doivent fournir chaque année au commissaire à l'information et à la protection de la vie privée de l'Ontario les rapports indiqués à l'article 34 de la LAIPVP. Chaque hôpital responsable de répondre à une demande d'accès ou à une demande de rectification concernant des dossiers de RPS dans le DSE doit inclure le nombre de demandes et de refus dans son rapport au commissaire à l'information et à la protection de la vie privée de l'Ontario même si cyberSanté Ontario a fourni les dossiers de RPS au demandeur au nom de l'hôpital.

4 Procédures

4.1 Procédures pour répondre à une demande d'accès

Demande directe de la personne pour des dossiers créés et versés uniquement par le DRS

4.1.1 Lorsqu'un DRS reçoit une demande d'accès directement d'une personne concernant des dossiers de RPS créés et versés dans le DSE uniquement par le DRS en question, le DRS doit respecter la Partie V de la LPRPS ainsi que ses politiques, ses procédures et ses pratiques internes pour répondre à la demande d'accès de la personne. Cela n'empêche pas un dépositaire de renseignements sur la santé ou l'agent d'un dépositaire de renseignements sur la santé, en réponse à une demande verbale d'accès, d'accorder à la personne un accès à un dossier de renseignements personnels sur la santé auquel elle a droit pendant que des soins de santé lui sont prodigués.

Demande directe de la personne pour des dossiers recueillis par le DRS

4.1.2 Lorsqu'un DRS reçoit une demande d'accès directement d'une personne concernant des dossiers de RPS recueillis par le DRS en question afin qu'on prodigue ou contribue à prodiguer à cette dernière des soins de santé, le DRS doit respecter la Partie V de la LPRPS ainsi que ses politiques, ses procédures et ses pratiques internes pour répondre à la demande d'accès de la personne. Cela n'empêche pas un dépositaire de renseignements sur la santé ou l'agent d'un dépositaire de renseignements sur la santé, en réponse à une demande verbale d'accès, d'accorder à la personne un accès à un dossier de renseignements personnels sur la santé auquel elle a droit pendant que des soins de santé lui sont prodigués.

Demande liée à des dossiers créés et versés par un autre DRS

4.1.3 Lorsqu'un DRS reçoit une demande d'accès directement d'une personne concernant des dossiers de RPS créés et versés au DSE par un ou plus d'un autre DRS et que le DRS qui a reçu la demande d'accès n'a pas recueilli de RPS, le DRS ayant reçu la demande d'accès doit, le plus tôt possible, faire ce qui suit :

- informer la personne du fait que la demande d'accès concerne des RPS qui ne sont pas sous la garde ou le contrôle du DRS qui a reçu la demande d'accès;
- fournir à la personne l'information lui permettant de communiquer avec cyberSanté Ontario pour formuler sa demande d'accès.

4.1.4 Lorsque cyberSanté Ontario reçoit une demande d'accès directement d'une personne concernant des dossiers de RPS créés et versés dans le DSE, il doit faire ce qui suit :

- vérifier l'identité de la personne qui fait la demande d'accès et confirmer qu'il s'agit bien de celle que concernent les dossiers de RPS dans le DSE faisant l'objet de la demande d'accès ou de son mandataire spécial;
- informer la personne du fait que la demande d'accès sera envoyée au DRS ou aux DRS qui ont créé et versé les dossiers de RPS dans le DSE;
- obtenir de la personne assez de renseignements pour que le DRS ou les DRS qui ont créé et versé les dossiers de RPS dans le DSE puissent identifier la personne dans le DSE, trouver ses RPS dans le DSE et donner suite à la demande d'accès;
- obtenir de la personne une adresse pour l'envoi de la réponse à la demande d'accès et d'autres coordonnées nécessaires selon les circonstances.

4.1.5 Sur demande de cyberSanté Ontario, les DRS doivent aider cyberSanté Ontario à vérifier l'identité de la personne qui fait la demande d'accès et à confirmer qu'il s'agit bien de celle que concernent les dossiers de RPS dans le DSE faisant l'objet de la demande d'accès ou de son mandataire spécial.

4.1.6 Le plus tôt possible, mais, en toute circonstance, au plus tard sept (7) jours après la réception de la demande d'accès directement de la personne que concernent les dossiers de RPS créés et versés dans le DSE, cyberSanté Ontario doit identifier le DRS ou les DRS qui ont créé et versé les dossiers de RPS dans le DSE faisant l'objet de la demande d'accès et transmettre la demande d'accès au DRS ou aux DRS identifiés.

Demande reçue par cyberSanté Ontario liée à des dossiers créés et versés par un DRS seulement

4.1.7 Lorsque la demande d'accès est liée à des dossiers de RPS créés et versés dans le DSE par un DRS seulement, cyberSanté Ontario doit faire ce qui suit :

- informer le DRS du fait qu'il est le seul à avoir créé et versé les dossiers de RPS dans le DSE faisant l'objet de la demande d'accès;
- fournir au DRS l'information reçue aux termes du paragraphe 4.1.4;
- informer le DRS du fait qu'il doit répondre directement à la personne concernant sa demande d'accès conformément à la Partie V de la LPRPS ainsi qu'à ses politiques, à ses procédures et à ses pratiques internes dans les trente (30) jours suivant la réception par cyberSanté Ontario de la demande d'accès de la personne.

4.1.8 Lorsqu'il reçoit une demande d'accès de cyberSanté Ontario concernant des dossiers de RPS qu'il est le seul à avoir créés et versés dans le DSE, le DRS doit respecter la Partie V de la LPRPS ainsi que ses politiques, ses procédures et ses pratiques internes pour répondre à la demande d'accès de la personne.

4.1.9 Le DRS doit, le plus tôt possible, enregistrer un journal indiquant qu'il a répondu à la demande d'accès.

Demande reçue par cyberSanté Ontario liée à des dossiers créés et versés par plus d'un DRS seulement

4.1.10 Lorsque la demande d'accès est liée à des dossiers de RPS créés et versés dans le DSE par plus d'un DRS seulement, cyberSanté Ontario doit faire ce qui suit :

- informer chaque DRS du fait que les dossiers de RPS faisant l'objet de la demande d'accès ont été créés et versés par plus d'un DRS;
- fournir à chaque DRS l'information reçue aux termes du paragraphe 4.1.4;
- indiquer à chaque DRS qu'il doit, le plus tôt possible, mais, en toute circonstance, au plus tard vingt et un (21) jours après la réception de la demande d'accès de cyberSanté Ontario, faire ce qui suit :
  - informer cyberSanté Ontario du fait que le DRS acceptera la demande d'accès en totalité ou en partie et fournir à cyberSanté Ontario les directives explicites pour répondre à la demande d'accès;
  - si le DRS accepte la demande d'accès en totalité ou en partie, fournir à cyberSanté Ontario une estimation des frais, le cas échéant, pour fournir l'accès aux dossiers de RPS;
  - si le DRS refuse la demande d'accès en totalité ou en partie, fournir à cyberSanté Ontario un avis écrit adressé à la personne et rédigé conformément à la Partie V de la LPRPS;
  - si le DRS prolonge le délai de réponse à la demande d'accès pour une période supplémentaire d'au plus trente (30) jours, fournir à cyberSanté Ontario un avis écrit adressé à la personne et rédigé conformément à la Partie V de la LPRPS.

4.1.11 Le plus tôt possible, mais, en toute circonstance, au plus tard vingt et un (21) jours après la réception de la demande d'accès de cyberSanté Ontario, le DRS doit faire ce qui suit :

- informer cyberSanté Ontario du fait que le DRS acceptera la demande d'accès en totalité ou en partie et fournir à cyberSanté Ontario les directives explicites pour répondre à la demande d'accès;

- si le DRS accepte la demande d'accès en totalité ou en partie, fournir à cyberSanté Ontario une estimation des frais, le cas échéant, pour fournir l'accès aux dossiers de RPS;
- si le DRS refuse la demande d'accès en totalité ou en partie, fournir à cyberSanté Ontario un avis écrit adressé à la personne et rédigé conformément à la Partie V de la LPRPS;
- si le DRS prolonge le délai de réponse à la demande d'accès pour une période supplémentaire d'au plus trente (30) jours, fournir à cyberSanté Ontario un avis écrit adressé à la personne et rédigé conformément à la Partie V de la LPRPS.

4.1.12 Lorsque le DRS ne répond pas à cyberSanté Ontario dans le délai prescrit au paragraphe 4.1.11, cyberSanté Ontario doit fournir un avis écrit à la personne mentionnant que le DRS n'a pas répondu à la demande d'accès et que la personne peut faire une plainte au DRS qui n'a pas répondu à la demande d'accès ou déposer une plainte auprès du commissaire à l'information et à la protection de la vie privée de l'Ontario.

4.1.13 Dans les trente (30) jours suivant la demande d'accès de la personne, cyberSanté Ontario doit, conformément à la Partie V de la LPRPS, faire ce qui suit :

- fournir à la personne une estimation des frais, le cas échéant, pour accorder l'accès aux dossiers de RPS pour lesquels la demande d'accès a été acceptée en totalité ou en partie;
- percevoir les frais, le cas échéant, au nom des DRS pour accorder l'accès aux dossiers de RPS pour lesquels la demande d'accès a été acceptée en totalité ou en partie;
- fournir à la personne une copie des dossiers de RPS pour lesquels la demande d'accès a été acceptée en totalité ou en partie;
- fournir à la personne les avis écrits nécessaires en cas de refus de la demande d'accès en totalité ou en partie;
- fournir à la personne les avis écrits nécessaires en cas de prolongation du délai pour répondre à la demande d'accès;
- fournir à la personne les avis écrits nécessaires aux termes du paragraphe 4.1.12.

4.1.14 Lorsqu'un avis écrit de prolongation du délai pour répondre à une demande d'accès a été fourni à la personne, le DRS qui demande la prolongation doit respecter la Partie V de la LPRPS ainsi que ses politiques, ses procédures et ses pratiques internes pour répondre directement à la personne concernant sa demande d'accès.

4.1.15 cyberSanté Ontario doit, le plus tôt possible, créer un journal mentionnant qu'il a répondu à la demande d'accès au nom des DRS qui ont créé et versé les dossiers de RPS dans le DSE à moins que le DRS n'ait pas répondu à cyberSanté Ontario concernant la demande d'accès dans le délai indiqué au paragraphe 4.1.11 ou ait prolongé le délai pour répondre à la demande d'accès. Tout DRS qui ne répond pas à cyberSanté Ontario concernant la demande d'accès dans le délai indiqué au paragraphe 4.1.11 ou qui prolonge le délai pour répondre à la demande d'accès doit créer, le plus tôt possible, un journal mentionnant qu'il a répondu à la demande d'accès.

Demande liée aux journaux

4.1.16 Le DRS doit respecter la Partie V de la LPRPS ainsi que ses politiques, ses procédures et ses pratiques internes pour répondre à la demande d'accès de la personne lorsqu'il reçoit une demande d'accès directement de cette personne concernant les dossiers suivants :

- les dossiers relatifs à tous les cas où la totalité ou une partie des RPS de la personne est consultée, manipulée ou autrement employée par les DRS ou leurs mandataires et leurs fournisseurs de services électroniques;
- les dossiers relatifs à tous les cas où une directive sur le consentement est formulée, modifiée ou retirée par la personne;
- les dossiers relatifs à tous les cas où on déroge à une directive sur le consentement formulée par la personne et la raison de la dérogation.

4.1.17 Lorsque le DRS recevant une demande d'accès liée aux dossiers indiqués au paragraphe 4.1.16 n'est pas en mesure de produire et de fournir des copies des dossiers pour répondre à la demande d'accès, il doit, le plus tôt possible, faire ce qui suit :

- informer la personne du fait que le DRS n'est pas en mesure de traiter la demande d'accès;
- fournir à la personne l'information lui permettant de communiquer avec cyberSanté Ontario pour formuler sa demande d'accès.

4.1.18 Lorsque cyberSanté Ontario reçoit une demande d'accès liée aux dossiers indiqués au paragraphe 4.1.16 directement d'une personne, il doit répondre directement à cette personne concernant la demande d'accès conformément à la Partie V de la LPRPS et à ses politiques, à ses procédures et à ses pratiques internes.

4.1.19 À la réception de la demande d'accès liée aux dossiers indiqués au paragraphe 4.1.16, cyberSanté Ontario doit faire ce qui suit :

- vérifier l'identité de la personne qui fait la demande d'accès et confirmer qu'il s'agit bien de celle que concernent les dossiers de RPS dans le DSE faisant l'objet de la demande d'accès ou de son mandataire spécial;
- obtenir de la personne assez de renseignements pour permettre à cyberSanté Ontario d'identifier la personne dans le DSE, de trouver ses RPS dans le DSE et de donner suite à la demande d'accès;
- obtenir de la personne une adresse pour l'envoi de la réponse à la demande d'accès et d'autres coordonnées nécessaires selon les circonstances;
- répondre directement à la personne concernant la demande d'accès conformément à la Partie V de la LPRPS et à ses politiques, à ses procédures et à ses pratiques internes;
- aviser la personne du fait que le DRS sera informé de la demande d'accès une fois qu'on aura donné suite à la demande.

4.1.20 Sur demande de cyberSanté Ontario, les DRS doivent aider cyberSanté Ontario à vérifier l'identité de la personne qui fait la demande d'accès et à confirmer qu'il s'agit bien de celle que concernent les dossiers de RPS dans le DSE faisant l'objet de la demande d'accès ou de son mandataire spécial.

4.1.21 cyberSanté Ontario doit, le plus tôt possible, enregistrer un journal indiquant qu'il a répondu à la demande d'accès liée aux dossiers indiqués au paragraphe 4.1.16.

4.2 Procédures pour exiger des frais d'accès

4.2.1 Les DRS peuvent exiger des frais pour accorder l'accès aux dossiers de RPS dans le DSE aux conditions suivantes :

- le DRS fournit d'abord une estimation des frais;
- les frais ne dépassent pas le montant raisonnable permettant de récupérer les coûts de l'accès;
- les frais respectent les ordonnances applicables du commissaire à l'information et à la protection de la vie privée de l'Ontario.

4.2.2 Les DRS peuvent déterminer à leur discrétion d'exonérer le paiement de la totalité ou de toute partie des frais conformément à la Partie V de la LPRPS et à leurs politiques, à leurs procédures et à leurs pratiques internes.

4.2.3 Lorsque la demande d'accès concerne des dossiers de RPS créés et versés au DSE par plus d'un DRS, cyberSanté Ontario a la responsabilité de recueillir l'estimation des frais demandés par les DRS ayant créé et versé les dossiers, de fournir l'estimation des frais à la personne, le cas échéant, et de percevoir les frais.

4.2.4 Lorsqu'une demande d'accès concerne des dossiers de RPS créés et versés au DSE par un seul DRS, ce dernier a la responsabilité de fournir une estimation des frais qu'il demande, le cas échéant, et de percevoir les frais.

4.2.5 cyberSanté Ontario n'exigera aucuns frais pour ses services de coordination des réponses aux demandes d'accès ou de réponse aux demandes d'accès liés aux dossiers de RPS dans le DSE.

4.3 Procédures pour répondre à une demande de rectification

Demande directe de la personne pour des dossiers créés et versés uniquement par le DRS

4.3.1 Lorsqu'un DRS reçoit une demande de rectification directement d'une personne concernant des dossiers de RPS créés et versés dans le DSE uniquement par le DRS en question, le DRS doit respecter la Partie V de la LPRPS ainsi que ses politiques, ses procédures et ses pratiques internes pour répondre à la demande de rectification de la personne.

4.3.2 Lorsque le DRS accepte la demande de rectification ou doit joindre un avis de rejet aux termes du paragraphe 55(11) de la LPRPS et que la demande de rectification ou l'avis de rejet concerne un dossier de RPS dans le DSE qui ne peut être rectifié directement par le DRS, ce dernier doit, le plus tôt possible, demander à cyberSanté Ontario d'apporter la rectification ou de joindre l'avis de rejet conformément à la Partie V de la LPRPS.

4.3.3 Le plus tôt possible, mais, en toute circonstance, au plus tard sept (7) jours après la réception de la demande du DRS, cyberSanté Ontario doit apporter la rectification nécessaire ou joindre l'avis de rejet conformément à la Partie V de la LPRPS.

4.3.4 Après avoir apporté la rectification demandée ou joint l'avis de rejet, cyberSanté Ontario doit, le plus tôt possible, informer le DRS du fait que cyberSanté Ontario a apporté la rectification demandée ou a joint l'avis de rejet et de la manière dont la rectification demandée a été apportée pour que le DRS respecte les obligations que lui impose l'article 55 de la LPRPS.

4.3.5 Après avoir accepté la demande de rectification, le DRS doit, conformément au paragraphe 55(10) de la LPRPS, faire ce qui suit :

- aviser la personne de ce qui a été fait pour effectuer la rectification demandée le plus tôt possible;
- à la demande de la personne, donner un avis écrit de la rectification demandée, dans la mesure du raisonnable, aux personnes à qui le DRS a divulgué les RPS le plus tôt possible, sauf si la rectification pourrait raisonnablement n'avoir aucun effet sur la prestation continue de soins de santé ou d'autres services à la personne.

4.3.6 Le DRS doit, le plus tôt possible, enregistrer un journal indiquant qu'il a répondu à la demande de rectification.

4.3.7 cyberSanté Ontario doit veiller à ce que le DSE conserve et affiche un historique de toutes les rectifications de dossiers de RPS dans le DSE, peu importe si la rectification a été réalisée par le DRS ou cyberSanté Ontario.

4.3.8 Les DRS et cyberSanté Ontario doivent veiller à ce que les rectifications de dossiers de RPS dans le DSE soient réalisées conformément au paragraphe 55(10) de la LPRPS.

Demande liée à des dossiers créés et versés par un autre DRS seulement ou plus d'un DRS

4.3.9 Lorsqu'un DRS reçoit une demande de rectification directement d'une personne concernant des dossiers de RPS créés et versés au DSE par seulement un autre DRS ou plus d'un DRS, le DRS ayant reçu la demande de rectification doit, le plus tôt possible, faire ce qui suit :

- informer la personne du fait que la demande de rectification concerne des RPS qui ne sont pas sous la garde ou le contrôle du DRS qui a reçu la demande de rectification;
- fournir à la personne l'information lui permettant de communiquer avec cyberSanté Ontario pour formuler sa demande de rectification.

4.3.10 Lorsque cyberSanté Ontario reçoit une demande de rectification directement d'une personne concernant des dossiers de RPS créés et versés dans le DSE par un ou plus d'un DRS, il doit faire ce qui suit :

- vérifier l'identité de la personne qui fait la demande de rectification et confirmer qu'il s'agit bien de celle que concernent les dossiers de RPS dans le DSE faisant l'objet de la demande de rectification ou de son mandataire spécial;
- informer la personne du fait que la demande de rectification sera envoyée au DRS ou aux DRS qui ont créé et versé les dossiers de RPS dans le DSE;
- obtenir de la personne assez de renseignements pour que le DRS ou les DRS qui ont créé et versé les dossiers de RPS dans le DSE puissent identifier la personne dans le DSE, trouver ses RPS dans le DSE et donner suite à la demande de rectification;
- obtenir de la personne une adresse pour l'envoi de la réponse à la demande de rectification et d'autres coordonnées nécessaires selon les circonstances.

4.3.11 Sur demande de cyberSanté Ontario, les DRS doivent aider cyberSanté Ontario à vérifier l'identité de la personne qui fait la demande de rectification et à confirmer qu'il s'agit bien de celle que concernent les dossiers de RPS dans le DSE faisant l'objet de la demande de rectification ou de son mandataire spécial.

4.3.12 Le plus tôt possible, mais, en toute circonstance, au plus tard sept (7) jours après la réception de la demande de rectification, cyberSanté Ontario doit identifier le DRS ou les DRS qui ont créé et versé les dossiers de RPS dans le DSE faisant l'objet de la demande de rectification et transmettre la demande de rectification à chaque DRS identifié.

4.3.13 En transmettant la demande de rectification, cyberSanté Ontario doit faire ce qui suit :

- fournir à chaque DRS l'information reçue aux termes du paragraphe 4.3.10;
- informer chaque DRS du fait qu'il doit répondre directement à la personne concernant la demande de rectification conformément à la Partie V de la LPRPS et à ses politiques, à ses procédures et à ses pratiques internes.

4.3.14 Lorsqu'il reçoit une demande de rectification de cyberSanté Ontario concernant des dossiers de RPS qu'il a lui-même créés et versés dans le DSE, le DRS doit respecter la Partie V de la LPRPS ainsi que ses politiques, ses procédures et ses pratiques pour répondre à la demande de rectification de la personne.

4.3.15 Lorsque le DRS accepte la demande de rectification ou doit joindre un avis de rejet aux termes du paragraphe 55(11) de la LPRPS et que la demande de rectification ou l'avis de rejet concerne un dossier de RPS dans le DSE qui ne peut être rectifié directement par le DRS, ce dernier doit, le plus tôt possible, demander à cyberSanté Ontario d'apporter la rectification ou de joindre l'avis de rejet conformément à la Partie V de la LPRPS.

4.3.16 Le plus tôt possible, mais, en toute circonstance, au plus tard sept (7) jours après la réception de la demande du DRS, cyberSanté Ontario doit apporter la rectification demandée ou joindre l'avis de rejet conformément à la Partie V de la LPRPS et informer le DRS du fait que cyberSanté Ontario a apporté la rectification demandée ou a joint l'avis de rejet et de la manière dont a été effectuée la rectification demandée pour que le DRS respecte les obligations que lui impose l'article 55 de la LPRPS.

4.3.17 Après avoir accepté la demande de rectification, le DRS doit, conformément au paragraphe 55(10) de la LPRPS, faire ce qui suit :

- aviser la personne de ce qui a été fait pour effectuer la rectification demandée le plus tôt possible;
- à la demande de la personne, donner un avis écrit de la rectification demandée, dans la mesure du raisonnable, aux personnes à qui le DRS a divulgué les RPS le plus tôt possible, sauf si la rectification pourrait raisonnablement n'avoir aucun effet sur la prestation continue de soins de santé ou d'autres services à la personne.

4.3.18 Le DRS doit, le plus tôt possible, enregistrer un journal indiquant qu'il a répondu à la demande de rectification.

4.3.19 cyberSanté Ontario doit veiller à ce que le DSE conserve et affiche un historique de toutes les rectifications de dossiers de RPS dans le DSE, peu importe si la rectification a été réalisée par le DRS ou cyberSanté Ontario.

4.3.20 Les DRS et cyberSanté Ontario doivent veiller à ce que les rectifications de dossiers de RPS dans le DSE soient réalisées conformément au paragraphe 55(10) de la LPRPS.

4.4 Plaintes liées aux demandes d'accès, aux demandes de rectification et aux frais

4.4.1 Toutes les plaintes concernant les demandes d'accès, les demandes de rectification et les frais pour répondre aux demandes d'accès doivent être traitées conformément à la *Politique sur les demandes de renseignements et les plaintes relatives au dossier de santé électronique* et aux procédures connexes, ce qui comprend les modifications qui y sont apportées de temps à autre.

5 Application[3]

5.1.1 Tous les cas de non-respect seront examinés par le comité de protection de la vie privée et de sécurité applicable. Le comité de protection de la vie privée et de sécurité applicable recommandera la voie à suivre à l'organisme de surveillance applicable.

L'organisme de surveillance applicable a le pouvoir d'imposer les sanctions appropriées, ce qui peut inclure la cessation des ententes applicables avec le DRS ou la cessation des privilèges d'accès des mandataires et des fournisseurs de services électroniques et une demande de mesures correctives.

6 Glossaire

Dossier de santé électronique (DSE)
Ensemble de la solution ConnexionOntario et du Dépôt des Services communs d'imagerie diagnostique, soit des dépôts ou des systèmes auxiliaires cliniques destinés à stocker et à rendre accessibles des renseignements personnels sur la santé contenus dans les systèmes électroniques de renseignements sur la santé des dépositaires de ces renseignements de manière à ne créer qu'un seul référentiel.

Fournisseur de services électroniques
Personne qui fournit des biens ou des services dans le but de permettre à un dépositaire de renseignements sur la santé d'employer des moyens électroniques de recueillir, d'utiliser, de modifier, de diffuser, de conserver ou d'éliminer des renseignements personnels sur la santé et qui comprend un fournisseur de réseau d'information sur la santé.

Demande d'accès
Demande formulée par une personne pour exercer son droit, conformément à la Partie V de la *Loi de 2004 sur la protection des renseignements personnels sur la santé*, d'accéder aux dossiers de renseignements personnels sur la santé la concernant qui sont sous la garde ou le contrôle d'un dépositaire de renseignements sur la santé.
Sans limiter la généralité de ce qui précède, une personne peut faire une demande d'accès pour les dossiers suivants concernant le dossier de santé électronique :

- les dossiers cliniques de la personne;

[3] Les références au comité de protection de la vie privée et de sécurité applicable et à l'organisme de surveillance applicable se trouvent au *Tableau 1 : Organismes administratifs applicables*.

- les dossiers relatifs à tous les cas où la totalité ou une partie des RPS de la personne est consultée, manipulée ou autrement employée par les DRS ou leurs mandataires et leurs fournisseurs de services électroniques;
- les dossiers relatifs à tous les cas où une directive sur le consentement est formulée, modifiée ou retirée par la personne;
- les dossiers relatifs à tous les cas où on déroge à une directive sur le consentement formulée par la personne et la raison de la dérogation.

Demande de rectification
Demande formulée par une personne pour exercer son droit, conformément à la Partie V de la *Loi de 2004 sur la protection des renseignements personnels sur la santé*, de demander une rectification des dossiers de renseignements personnels sur la santé la concernant qu'elle juge inexacts ou incomplets aux fins auxquelles les renseignements personnels sur la santé ont été recueillis ou utilisés ou sont utilisés.

Structure d'administration de la politique	Solution ConnexionOntario	Dépôt des Services communs d'imagerie diagnostique
Comité de protection de la vie privée et de sécurité applicable	Protection de la vie privée : Comité de protection de la vie privée (Connecting Privacy) Sécurité : Comité de sécurité (Connecting Security)	Protection de la vie privée : Groupe de travail sur la protection de la vie privée et la sécurité des Services communs d'imagerie diagnostique Sécurité : Comité de sécurité (Connecting Security)
Organisme de surveillance applicable	Protection de la vie privée : Comité directeur de ConnexionOntario Sécurité : Comité stratégique de cyberSanté Ontario	Protection de la vie privée : Comité exécutif des Services communs d'imagerie diagnostique Sécurité : Comité stratégique de cyberSanté Ontario

Tableau 1 : Organismes administratifs applicables

Terme ou sigle	Définition
DRS	Dépositaire de renseignements sur la santé
RPS	Renseignements personnels sur la santé, tel que le terme est défini dans la *Loi de 2004 sur la protection des renseignements personnels sur la santé*
LPRPS	*Loi de 2004 sur la protection des renseignements personnels sur la santé*

7 Références et documents connexes

Loi de 2004 sur la protection des renseignements personnels sur la santé (LPRPS)
Commissaire à l'information et à la protection de la vie privée de l'Ontario, ordonnance HO-009
Politique sur les demandes de renseignements et les plaintes relatives au dossier de santé électronique et procédures connexes

eHealth Ontario

Politique de vérification de la conformité

Dossier de santé électronique

Version : 2.0

N° de document : 3874

Ontario
eHealth Ontario

Gestion du document

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

Historique des approbations

APPROBATEURS	DATE D'APPROBATION
Membres du comité de protection de la vie privée ConnectingPrivacy	8 décembre 2016

Historique des révisions

NUMÉRO DE VERSION	DATE AAAA-MM-JJ	RÉSUMÉ DES CHANGEMENTS	AUTEUR DES CHANGEMENTS
2.0	2016-12-01	Révisions conformément à l'évaluation des politiques par le CPC	Rand Muhtam, analyste en protection de la vie privée, cyberSanté Ontario
1.1	2015-11-25	Révisions mineures – mise à jour pour ConnexionOntario	Samara Strub, analyste en protection de la vie privée, cyberSanté Ontario
1.0	2014-11-17	Version définitive	Urooj Kirmani, analyste principal en protection de la vie privée, cyberSanté Ontario
0.01	2014-11-04	Première version établie en fonction de la politique harmonisée sur la vérification du comité de protection de la vie privée ConnectingPrivacy, v1.3	Promila Gonsalves, analyste en protection de la vie privée, cyberSanté Ontario

Table des matières

1 Objectif

Le présent document définit les politiques, les procédures et les pratiques que les dépositaires de renseignements sur la santé (DRS) et cyberSanté Ontario doivent avoir en place pour vérifier si les DRS et cyberSanté Ontario respectent les obligations imposées par la *Loi de 2004 sur la protection des renseignements personnels sur la santé* (LPRPS), les ententes applicables ainsi que les politiques, les procédures et les pratiques en vigueur concernant le dossier de santé électronique (DSE).

2 Portée

La présente politique et les procédures connexes s'appliquent à la conduite de cyberSanté Ontario, des DRS qui créent et versent ou collectent, utilisent ou divulguent des renseignements personnels sur la santé (RPS) dans le DSE et les mandataires et les fournisseurs de services électroniques des DRS ou de cyberSanté Ontario. Le DSE est composé de la solution ConnexionOntario et du Dépôt des Services communs d'imagerie diagnostique. La solution ConnexionOntario et le Dépôt des Services communs d'imagerie diagnostique sont des dépôts ou des systèmes auxiliaires cliniques destinés à stocker et à rendre accessibles des renseignements personnels sur la santé contenus dans les systèmes électroniques de renseignements sur la santé des dépositaires de ces renseignements[1].

3 Politique

3.1 Fondements

3.1.1 Les DRS et cyberSanté Ontario doivent avoir en place les politiques, les procédures et les pratiques sur la protection de la vie privée et la sécurité nécessaires pour les rendre conformes à leurs obligations aux termes de la LPRPS, des ententes applicables et de la présente politique ainsi que des procédures connexes.

3.1.2 Les DRS et cyberSanté Ontario doivent harmoniser les ententes applicables ainsi que les politiques, les procédures et les pratiques en vigueur concernant le DSE.

3.1.3 Les DRS et cyberSanté Ontario doivent avoir en place des politiques, des procédures et des pratiques sur la protection de la vie privée et la sécurité qui respectent la LPRPS et informer leurs mandataires et leurs fournisseurs de services électroniques sur les politiques, les procédures et les pratiques imposées par la LPRPS.

3.1.4 Les DRS et cyberSanté Ontario doivent prendre les mesures nécessaires et raisonnables selon les circonstances afin que leurs mandataires et leurs fournisseurs de services électroniques se conforment à la LPRPS, aux ententes applicables ainsi qu'aux politiques, aux procédures et aux pratiques en vigueur concernant le DSE.

3.1.5 Les DRS doivent cerner et atténuer les risques à la confidentialité et à la sécurité et résoudre les éléments non conformes[2] concernant le DSE, notamment par des auto-évaluations de leur préparation en matière de confidentialité et de sécurité (le cas échéant), des auto-attestations opérationnelles en matière de confidentialité et de sécurité, des activités de vérification et de surveillance ainsi que la vérification de la conformité des mandataires et des fournisseurs de services électroniques.

---

[1] Les divergences entre les exigences des politiques et des procédures de la solution ConnexionOntario et du Dépôt des Services communs d'imagerie diagnostique sont indiquées dans la présente politique.

[2] Aux fins de la présente politique et des procédures connexes, le terme *éléments non conformes* fait référence au non-respect de la LPRPS, des ententes applicables et des politiques, des procédures et des pratiques en vigueur concernant le DSE.

3.1.6 cyberSanté Ontario doit cerner et atténuer les risques à la confidentialité et à la sécurité et résoudre les éléments non conformes concernant le DSE, notamment par des évaluations des conséquences sur la vie privée, des auto-évaluations de sa préparation en matière de confidentialité et de sécurité (le cas échéant), des auto-attestations opérationnelles en matière de confidentialité et de sécurité, des activités de vérification et de surveillance ainsi que la vérification de la conformité des mandataires, des fournisseurs de services électroniques et des tiers.

3.1.7 Les DRS et cyberSanté Ontario doivent signaler tout risque à la confidentialité ou à la sécurité et tout élément non conforme qui pourrait avoir des conséquences sur la vie privée de personnes ou la sécurité de leurs RPS dans le DSE au comité de protection de la vie privée et de sécurité applicable.

3.1.8 Les DRS et cyberSanté Ontario doivent se conformer aux décisions et aux directives de l'organisme de surveillance applicable et coopérer en cas de vérification effectuée par le comité de protection de la vie privée et de sécurité applicable aux termes de la présente politique et des procédures connexes.

4 Procédures

4.1 Procédures pour les évaluations des conséquences sur la vie privée

4.1.1 cyberSanté Ontario doit surveiller et déterminer le comité de protection de la vie privée et de sécurité applicable et lui fournir un rapport écrit le plus tôt possible après la mise au jour d'au moins l'une des circonstances suivantes concernant le DSE :

- une nouvelle source de RPS;
- de nouveaux types ou rôles de DRS ou de mandataires de DRS qui recueillent, utilisent ou divulguent des RPS;
- de nouveaux types ou rôles de cyberSanté Ontario ou de fournisseurs de services électroniques qui consultent, manipulent ou traitent des RPS;
- de nouvelles manières de recueillir, d'utiliser ou de divulguer des RPS par les DRS ou leurs mandataires;
- de nouvelles manières de consulter, de manipuler ou de traiter des RPS par cyberSanté Ontario ou des fournisseurs de services électroniques;
- des changements à l'architecture frontale et dorsale existante ou à une fonctionnalité qui pourraient avoir des conséquences sur la vie privée de personnes ou la sécurité de leurs RPS;
- des changements au modèle de soutien opérationnel ou aux systèmes, aux processus ou aux parties qui pourraient avoir des conséquences sur la vie privée de personnes ou la sécurité de leurs RPS;
- des changements aux ententes applicables qui pourraient avoir des conséquences sur la vie privée de personnes ou la sécurité de leurs RPS;
- des changements législatifs à la LPRPS qui pourraient avoir des conséquences sur la vie privée de personnes ou la sécurité de leurs RPS;
- un élément vulnérable qui pourrait entraîner une atteinte à la confidentialité au sens de la *Politique de gestion des atteintes à la confidentialité du dossier de santé électronique* et des procédures connexes, ce qui comprend les modifications qui y sont apportées de temps à autre.

4.1.2 Le rapport écrit indiqué au paragraphe 4.1.1 doit contenir les éléments suivants :

- une description des circonstances et des conséquences des circonstances sur la vie privée de personnes ou la sécurité de leurs RPS;
- une recommandation sur la pertinence pour cyberSanté Ontario de réaliser ou de réviser une évaluation des conséquences sur la vie privée (ECVP).

4.1.3 Le comité de protection de la vie privée et de sécurité applicable doit, à sa réunion suivant la réception du rapport aux termes du paragraphe 4.1.2, examiner le rapport et le fournir, en compagnie de sa recommandation écrite sur la pertinence pour cyberSanté Ontario d'effectuer ou de réviser une ECVP, à l'organisme de surveillance applicable pour que ce dernier l'étudie à sa prochaine réunion.

4.1.4 L'organisme de surveillance applicable doit, à sa réunion suivant la réception du rapport et de la recommandation exigés au paragraphe 4.1.3, faire ce qui suit :

- examiner le rapport et la recommandation reçus;
- rédiger sa décision quant à la pertinence pour cyberSanté Ontario de réaliser ou de réviser une ECVP;
- lorsqu'il est déterminé qu'une ECVP doit être réalisée ou révisée, formuler des directives par écrit à cyberSanté Ontario, ce qui comprend le délai accordé pour réaliser ou réviser l'ECVP;
- fournir une copie de la décision et des directives à cyberSanté Ontario et au comité de protection de la vie privée et de sécurité applicable.

4.1.5 cyberSanté Ontario doit se conformer à la décision et aux directives de l'organisme de surveillance applicable et fournir des mises au point par écrit sur l'état de l'ECVP à chaque réunion du comité de protection de la vie privée et de sécurité applicable.

4.1.6 Le comité de protection de la vie privée et de sécurité applicable doit surveiller la conformité de cyberSanté Ontario à la décision et aux directives de l'organisme de surveillance applicable et peut demander d'autres preuves de cette conformité. cyberSanté Ontario doit se conformer avec toute demande de preuves de conformité de la part du comité de protection de la vie privée et de sécurité applicable.

4.1.7 cyberSanté Ontario doit réaliser des évaluations des risques et des menaces (ERM) en fonction des circonstances et conformément à la *Politique de gestion des menaces et des risques relatifs au dossier de santé électronique* et aux procédures connexes, ce qui comprend les modifications qui y sont apportées de temps à autre.

4.1.8 Le comité de protection de la vie privée et de sécurité applicable doit établir les critères à suivre par cyberSanté Ontario pour déterminer si la gravité de chaque risque à la confidentialité et à la sécurité et de chaque élément non conforme cerné dans une ECVP est élevée, moyenne ou faible. L'organisme de surveillance applicable doit être consulté par le comité de protection de la vie privée et de sécurité applicable pour l'établissement des critères.

4.1.9 cyberSanté Ontario doit faire ce qui suit :

- attribuer une cote à chaque risque à la confidentialité et à la sécurité et à chaque élément non conforme mis au jour dans une ECVP aux termes du paragraphe 4.1.8;
- élaborer un plan d'atténuation des risques[3];
- veiller à ce que le plan d'atténuation des risques comprenne des mesures pour atténuer les risques à la confidentialité et à la sécurité et les éléments non conformes ayant une cote « élevé »;
- veiller à ce que le plan d'atténuation des risques comprenne des mesures pour atténuer les risques à la confidentialité et à la sécurité et les éléments non conformes ayant une cote « moyen » ou « faible » ou donner les raisons pour lesquelles on n'atténuera pas un ou plus d'un de ces risques à la confidentialité ou à la sécurité et de ces éléments non conformes.

4.1.10 cyberSanté Ontario doit compléter les ECVP au cours de la phase de définition du concept et examiner et réviser les ECVP et les ERM au besoin pendant la phase de conception détaillée et la phase de mise en œuvre.

4.1.11 cyberSanté Ontario doit, le plus tôt possible, mais, en toute circonstance, au plus tard trente (30) jours après avoir terminé ou révisé une ECVP, fournir au comité de protection de la vie privée et de sécurité applicable les éléments suivants :

- une copie de l'ECVP;
- la cote attribuée à chaque risque à la confidentialité et à la sécurité et à chaque élément non conforme cerné;
- le plan d'atténuation des risques;

[3] Aux fins de la présente politique et des procédures connexes, le plan d'atténuation des risques doit comprendre, au minimum, les mesures visant à atténuer les risques à la confidentialité et à la sécurité et les éléments non conformes mis au jour ainsi que le délai donné et les personnes responsables pour mettre en œuvre les mesures.

- une mention des raisons pour lesquelles on n'atténuera pas un ou plus d'un risque à la confidentialité et à la sécurité et élément non conforme auquel on a attribué une cote « moyen » ou « faible ».

4.1.12 Le comité de protection de la vie privée et de sécurité applicable doit, le plus tôt possible, mais, en toute circonstance, au plus tard à sa réunion suivant la réception de l'information demandée au paragraphe 4.1.11, faire ce qui suit :

- examiner l'information reçue;
- veiller à ce que tous les risques à la confidentialité et à la sécurité et les éléments non conformes aient été cernés;
- veiller à ce que la cote attribuée à chaque risque à la confidentialité et à la sécurité et à chaque élément non conforme cerné soit conforme au paragraphe 4.1.8;
- veiller à ce que le plan d'atténuation des risques propose une solution adéquate aux risques à la confidentialité et à la sécurité et aux éléments non conformes ayant une cote « élevé »;
- veiller à ce que le plan d'atténuation des risques propose une solution adéquate aux risques à la confidentialité et à la sécurité et aux éléments non conformes ayant une cote « moyen » ou « faible » ou donner les raisons pour lesquelles on n'atténuera pas un ou plus d'un de ces risques à la confidentialité ou à la sécurité et de ces éléments non conformes;
- présenter une recommandation écrite visant l'approbation de l'ECVP et du plan d'atténuation ou fournir des directives écrites à cyberSanté Ontario pour modifier l'ECVP et le plan d'atténuation et en présenter une version révisée et fournir le délai à rspecter pour la modification et la présentation de la version révisée;
- fournir une copie de ces directives à cyberSanté Ontario;
- fournir l'information reçue aux termes du paragraphe 4.1.11 avec les recommandations écrites qui l'accompagnent à l'organisme de surveillance applicable.

4.1.13 L'organisme de surveillance applicable de cyberSanté Ontario doit modifier et soumettre de nouveau l'ECVP et le plan d'atténuation au comité de protection de la vie privée et de sécurité applicable à des fins de recommandation de l'approbation dans les délais indiqués dans les instructions écrites en vertu du paragraphe 4,1,12, lorsqu'on lui demande de le faire.

4.1.14 L'organisme de surveillance applicable doit, le plus tôt possible, mais, en toute circonstance, au plus tard à sa réunion suivant la réception de l'information et des recommandations demandées au paragraphe 4.1.12, faire ce qui suit :

- examiner l'information et les recommandations reçues;
- veiller à ce que tous les risques à la confidentialité et à la sécurité et les éléments non conformes aient été cernés;
- veiller à ce que la cote attribuée à chaque risque à la confidentialité et à la sécurité et à chaque élément non conforme cerné soit conforme au paragraphe 4.1.8;
- veiller à ce que le plan d'atténuation des risques propose une solution adéquate aux risques à la confidentialité et à la sécurité et aux éléments non conformes ayant une cote « élevé »;
- veiller à ce que le plan d'atténuation des risques propose une solution adéquate aux risques à la confidentialité et à la sécurité et aux éléments non conformes ayant une cote « moyen » ou « faible » ou donner les raisons pour lesquelles on n'atténuera pas un ou plus d'un de ces risques à la confidentialité ou à la sécurité et de ces éléments non conformes;
- mettre une décision par écrit visant l'acceptation des risques à la confidentialité et à la sécurité et des éléments non conformes ayant reçu une cote « moyen » ou « faible » pour lesquels on ne propose aucune mesure d'atténuation ou fournir des directives écrites à cyberSanté Ontario pour modifier le plan d'atténuation des risques et ainsi proposer une solution aux risques à la confidentialité et à la sécurité et aux éléments non conformes concernés;
- mettre une décision par écrit visant l'approbation de l'ECVP et du plan d'atténuation des risques ou fournir des directives écrites à cyberSanté Ontario pour modifier l'ECVP et le plan d'atténuation des risques et en présenter une version révisée et fournir le délai à respecter pour la modification et la présentation de la version révisée;
- fournir une copie de la décision et des directives à cyberSanté Ontario et au comité de protection de la vie privée et de sécurité applicable.

4.1.15 cyberSanté Ontario doit modifier l'ECVP et le plan d'atténuation des risques et en soumettre une version révisée à l'approbation de l'organisme de surveillance applicable dans le délai établi dans les directives écrites fournies aux termes du paragraphe 4.1.13 lorsqu'il reçoit la directive de le faire.

4.1.16 cyberSanté Ontario doit, à l'approbation de l'ECVP et du plan d'atténuation des risques par l'organisme de surveillance applicable, faire ce qui suit :

- fournir une copie de l'ECVP ainsi qu'une copie du plan d'atténuation des risques à chaque DRS qui crée et verse ou recueille, utilise ou divulgue des RPS dans le DSE;
- mettre en œuvre le plan d'atténuation des risques;
- faire le point sur l'état de la mise en œuvre du plan d'atténuation des risques à chaque réunion du comité de protection de la vie privée et de sécurité applicable;
- fournir une mention écrite du comité de protection de la vie privée et de sécurité applicable attestant que le plan d'atténuation des risques a été entièrement mis en œuvre le plus tôt possible, mais, en toute circonstance, au plus tard trente (30) jours après la mise en œuvre.

4.1.17 Le comité de protection de la vie privée et de sécurité applicable doit surveiller la conformité de cyberSanté Ontario à la mise en œuvre du plan d'atténuation des risques approuvé par l'organisme de surveillance applicable et peut exiger d'autres preuves de conformité. cyberSanté Ontario doit se conformer à toute demande de preuves de conformité par le comité de protection de la vie privée et de sécurité applicable.

Solution ConnexionOntario seulement

4.2 Procédures pour l'auto-évaluation de la préparation en matière de confidentialité et de sécurité

4.2.1 Le comité de protection de la vie privée et de sécurité applicable doit établir les éléments suivants :

- les exigences de l'auto-évaluation de la préparation en matière de confidentialité et de sécurité servant à évaluer la préparation en matière de confidentialité et de sécurité et à cerner les risques à la confidentialité et à la sécurité et les éléments non conformes imposées par cyberSanté Ontario et les DRS qui créent et versent ou recueillent, utilisent ou divulguent les RPS dans le DSE;
- une indication selon laquelle l'incapacité de satisfaire à chaque exigence est un risque élevé, moyen ou faible.

4.2.2 Le comité de protection de la vie privée et de sécurité applicable doit créer, conserver et administrer l'auto-évaluation de la préparation en matière de confidentialité et de sécurité pour cyberSanté Ontario.

4.2.3 cyberSanté Ontario doit créer, conserver et administrer les auto-évaluations de la préparation en matière de confidentialité et de sécurité pour chaque DRS qui crée et verse ou recueille, utilise ou divulgue des RPS dans le DSE.

4.2.4 Le plus tôt possible, mais, en toute circonstance, avant la consultation, la manipulation ou le traitement de RPS par cyberSanté Ontario ou avant la collecte ou le versement ou l'utilisation ou la divulgation par un DRS de RPS dans le DSE, cyberSanté Ontario ou le DSR, selon le cas, doit faire ce qui suit :

- effectuer l'auto-évaluation de la préparation en matière de confidentialité et de sécurité;
- attribuer une cote à chaque risque à la confidentialité et à la sécurité et à chaque élément non conforme mis au jour dans une auto-évaluation de la préparation en matière de confidentialité et de sécurité aux termes du paragraphe 4.2.1;
- élaborer un plan d'atténuation des risques;
- veiller à ce que le plan d'atténuation des risques comprenne des mesures pour atténuer les risques à la confidentialité et à la sécurité et les éléments non conformes ayant une cote « élevé »;
- veiller à ce que le plan d'atténuation des risques comprenne des mesures pour atténuer les risques à la confidentialité et à la sécurité et les éléments non conformes ayant une cote « moyen » ou « faible » ou donner les raisons pour lesquelles on n'atténuera pas un ou plus d'un de ces risques à la confidentialité ou à la sécurité et de ces éléments non conformes;
- veiller à ce qu'un haut placé appose sa signature sur l'auto-évaluation de la préparation en matière de confidentialité et de sécurité et le plan d'atténuation des risques.

4.2.5 Le plus tôt possible, mais, en toute circonstance, avant la consultation, la manipulation ou le traitement de RPS par cyberSanté Ontario ou avant la collecte ou le versement ou l'utilisation ou la divulgation par un DRS de RPS dans le DSE, cyberSanté Ontario ou le DSR, selon le cas, doit fournir au comité de protection de la vie privée et de sécurité applicable une copie de l'auto-évaluation de la préparation en matière de confidentialité et de sécurité effectuée.

4.3 Procédures pour l'auto-attestation opérationnelle en matière de confidentialité et de sécurité

4.3.1 Le comité de protection de la vie privée et de sécurité applicable doit établir les éléments suivants :

- les exigences de l'auto-attestation opérationnelle en matière de confidentialité et de sécurité servant à évaluer les activités permanentes en matière de confidentialité et de sécurité et à cerner les risques à la confidentialité et à la sécurité et les éléments non conformes imposées par cyberSanté Ontario et les DRS qui créent et versent ou recueillent, utilisent ou divulguent les RPS dans le DSE;
- une indication selon laquelle l'incapacité de satisfaire à chaque exigence est un risque élevé, moyen ou faible;
- une période au cours de laquelle, chaque année, l'auto-attestation opérationnelle en matière de confidentialité et de sécurité doit être administrée et effectuée.

4.3.2 Le comité de protection de la vie privée et de sécurité applicable doit créer, conserver et administrer l'auto-attestation opérationnelle en matière de confidentialité et de sécurité pour cyberSanté Ontario.

4.3.3 cyberSanté Ontario doit créer, conserver et administrer les auto-attestations opérationnelles en matière de confidentialité et de sécurité pour chaque DRS qui crée et verse ou recueille, utilise ou divulgue des RPS dans le DSE.

4.3.4 À la période précisée chaque année par le comité de protection de la vie privée et de sécurité applicable aux termes du paragraphe 4.3.1, cyberSanté Ontario et les DRS qui créent et versent ou recueillent, utilisent ou divulguent des RPS dans le DSE doivent faire ce qui suit :

- effectuer l'auto-attestation opérationnelle en matière de confidentialité et de sécurité;
- attribuer une cote à chaque risque à la confidentialité et à la sécurité et à chaque élément non conforme mis au jour dans une auto-attestation opérationnelle en matière de confidentialité et de sécurité aux termes du paragraphe 4.3.1;
- élaborer un plan d'atténuation des risques;
- veiller à ce que le plan d'atténuation des risques comprenne des mesures pour atténuer les risques à la confidentialité et à la sécurité et les éléments non conformes ayant une cote « élevé »;
- veiller à ce que le plan d'atténuation des risques comprenne des mesures pour atténuer les risques à la confidentialité et à la sécurité et les éléments non conformes ayant une cote « moyen » ou « faible » ou donner les raisons pour lesquelles on n'atténuera pas un ou plus d'un de ces risques à la confidentialité ou à la sécurité et de ces éléments non conformes;
- veiller à ce qu'un haut placé appose sa signature sur l'auto-attestation opérationnelle en matière de confidentialité et de sécurité et le plan d'atténuation des risques.

4.3.5 Le plus tôt possible, mais, en toute circonstance, au plus tard trente (30) jours après la période convenue aux termes du paragraphe 4.3.1, cyberSanté Ontario et les DRS qui créent et versent ou recueillent, utilisent ou divulguent des RPS dans le DSE doivent fournir au comité de protection de la vie privée et de sécurité applicable les éléments suivants :

- une copie de l'auto-attestation opérationnelle en matière de confidentialité et de sécurité effectuée;
- la cote attribuée à chaque risque à la confidentialité et à la sécurité et à chaque élément non conforme cerné;
- le plan d'atténuation des risques.

4.3.6 Le comité de protection de la vie privée et de sécurité applicable doit, le plus tôt possible, mais, en toute circonstance, au plus tard à sa réunion suivant la réception de l'information demandée au paragraphe 4.3.5, faire ce qui suit :

- examiner l'information reçue;

- solliciter les commentaires de cyberSanté Ontario concernant l'information fournie par un DRS aux termes du paragraphe 4.3.5;
- veiller à ce que tous les risques à la confidentialité et à la sécurité et les éléments non conformes aient été cernés;
- veiller à ce que la cote attribuée à chaque risque à la confidentialité et à la sécurité et à chaque élément non conforme cerné soit conforme au paragraphe 4.3.1;
- veiller à ce que le plan d'atténuation des risques satisfasse aux exigences du paragraphe 4.3.4;
- mettre une décision par écrit visant l'approbation de l'auto-attestation opérationnelle en matière de confidentialité et de sécurité et du plan d'atténuation des risques ou fournir des directives écrites à cyberSanté Ontario ou au DRS, selon le cas, pour modifier l'auto-attestation opérationnelle en matière de confidentialité et de sécurité et le plan d'atténuation des risques et en présenter une version révisée et fournir le délai à respecter pour la modification et la présentation de la version révisée;
- fournir une copie de la décision et des directives à cyberSanté Ontario ou au DRS, selon le cas;
- fournir l'information reçue aux termes du paragraphe 4.3.5, les commentaires reçus de cyberSanté Ontario, s'il y a lieu, ainsi que les recommandations écrites de ce dernier à l'organisme de surveillance applicable.

4.3.7 cyberSanté Ontario ou le DRS, selon le cas, doit modifier l'auto-attestation opérationnelle en matière de confidentialité et de sécurité et le plan d'atténuation des risques et en soumettre une version révisée à l'approbation de l'organisme de surveillance applicable dans le délai établi dans les directives écrites fournies aux termes du paragraphe 4.3.7 lorsqu'il reçoit la directive de le faire.

4.3.8 L'organisme de surveillance applicable doit, le plus tôt possible, mais, en toute circonstance, au plus tard à sa réunion suivant la réception de l'information et des recommandations demandées au paragraphe 4.3.6, faire ce qui suit :

- examiner l'information et les recommandations reçues;
- veiller à ce que tous les risques à la confidentialité et à la sécurité et les éléments non conformes aient été cernés;
- veiller à ce que la cote attribuée à chaque risque à la confidentialité et à la sécurité et à chaque élément non conforme cerné soit conforme au paragraphe 4.3.1;
- veiller à ce que le plan d'atténuation des risques satisfasse aux exigences du paragraphe 4.3.4;
- mettre une décision par écrit visant l'acceptation des risques à la confidentialité et à la sécurité et des éléments non conformes ayant reçu une cote « moyen » ou « faible » pour lesquels on ne propose aucune mesure d'atténuation ou fournir des directives écrites à cyberSanté Ontario ou au DRS, selon le cas, pour modifier le plan d'atténuation des risques et ainsi proposer une solution aux risques à la confidentialité et à la sécurité et aux éléments non conformes concernés;
- fournir une copie de la décision et des directives à cyberSanté Ontario ou au DRS, selon le cas, pour modifier l'auto-attestation opérationnelle en matière de confidentialité et de sécurité et le plan d'atténuation des risques et en présenter une version révisée et fournir le délai à respecter pour la modification et la présentation de la version révisée;
- fournir une copie de la décision et des directives à cyberSanté Ontario ou au DRS, selon le cas, et au comité de protection de la vie privée et de sécurité applicable.

4.3.9 cyberSanté Ontario ou le DRS, selon le cas, doit, à l'approbation de l'auto-attestation opérationnelle en matière de confidentialité et de sécurité et du plan d'atténuation des risques par l'organisme de surveillance applicable, faire ce qui suit :

- mettre en œuvre le plan d'atténuation des risques;
- faire le point sur l'état de la mise en œuvre du plan d'atténuation des risques à chaque réunion du comité de protection de la vie privée et de sécurité applicable;
- fournir une mention écrite du comité de protection de la vie privée et de sécurité applicable attestant que le plan d'atténuation des risques a été entièrement mis en œuvre le plus tôt possible, mais, en toute circonstance, au plus tard trente (30) jours après la mise en œuvre.

4.3.10 Le comité de protection de la vie privée et de sécurité applicable doit surveiller la conformité de cyberSanté Ontario ou du DRS, selon le cas, à la mise en œuvre du plan d'atténuation des risques approuvé par l'organisme de surveillance applicable et peut exiger d'autres preuves de conformité. cyberSanté Ontario ou le DRS, selon le cas, doit se conformer à toute demande de preuves de conformité par le comité de protection de la vie privée et de sécurité applicable.

4.4 Vérification de la conformité des mandataires, des fournisseurs de services électroniques et des tiers

4.4.1 cyberSanté Ontario doit veiller, y compris en mettant en place une politique, à ce que tout mandataire, fournisseur de services électroniques et tiers à qui il fait appel pour fournir des services concernant le DSE respecte les restrictions et les conditions permettant à cyberSanté Ontario de se conformer à la LPRPS, aux ententes applicables ainsi qu'aux politiques, aux procédures et aux pratiques en vigueur concernant le DSE.

4.4.2 Les DRS doivent prendre les mesures nécessaires et raisonnables selon les circonstances afin que leurs mandataires et leurs fournisseurs de services électroniques se conforment à la LPRPS, aux ententes applicables ainsi qu'aux politiques, aux procédures et aux pratiques en vigueur concernant le DSE.

4.5 Vérification et surveillance

4.5.1 cyberSanté Ontario et les DRS qui créent et versent ou recueillent, utilisent ou divulguent des RPS dans le DSE doivent effectuer la vérification et la surveillance des activités liées au DSE conformément à la LPRPS, aux ententes applicables ainsi qu'aux politiques, aux procédures et aux pratiques en vigueur concernant le DSE, ce qui comprend la *Politique pour la journalisation et la vérification du dossier de santé électronique*, la *Politique de gestion des atteintes à la confidentialité du dossier de santé électronique* et la *Politique pour la journalisation et la surveillance du dossier de santé électronique* ainsi que les procédures connexes avec les modifications qui y sont apportées de temps à autre.

4.5.2 cyberSanté Ontario et les DRS qui créent et versent ou recueillent, utilisent ou divulguent des RPS dans le DSE doivent, à la première occasion raisonnable, signaler au comité de protection de la vie privée et de sécurité applicable tout risque à la confidentialité ou à la sécurité ou tout élément non conforme qui pourrait avoir des conséquences sur la vie privée de personnes ou la sécurité de leurs RPS dans le DSE qui n'est pas indiqué dans les ECVP, les auto-évaluations de la préparation en matière de confidentialité et de sécurité et les auto-attestations opérationnelles en matière de confidentialité et de sécurité.

4.5.3 Le comité de protection de la vie privée et de sécurité applicable doit déterminer si des risques à la confidentialité ou à la sécurité ou des éléments non conformes qui pourraient avoir des conséquences sur la vie privée de personnes ou la sécurité de leurs RPS dans le DSE relevés par les ECVP, les auto-évaluations de la préparation en matière de confidentialité et de sécurité et les auto-attestations opérationnelles en matière de confidentialité et de sécurité pourraient exiger une vérification de la part du comité de protection de la vie privée et de sécurité applicable.

4.5.4 Le comité de protection de la vie privée et de sécurité applicable doit, le plus tôt possible, mais, en toute circonstance, au plus tard à sa réunion suivant la réception du rapport indiqué au paragraphe 4.5.2 ou la détermination des risques à la confidentialité et à la sécurité ou des éléments non conformes aux termes du paragraphe 4.5.3, faire ce qui suit :

- solliciter les commentaires de cyberSanté Ontario ou du DRS qu'on soupçonne à l'origine des risques à la confidentialité ou à la sécurité ou qu'on soupçonne non conforme, selon le cas;
- déterminer s'il y a des risques à la confidentialité ou à la sécurité ou des éléments non conformes qui pourraient avoir des conséquences sur la vie privée de personnes ou la sécurité de leurs RPS dans le DSE;
- déterminer si cyberSanté Ontario ou le DRS qu'on soupçonne à l'origine des risques à la confidentialité ou à la sécurité ou qu'on soupçonne non conforme, selon le cas, a mis ou mettra en œuvre des mesures pour atténuer les risques à la confidentialité et à la sécurité ou les éléments non conformes;
- déterminer s'il faut effectuer une vérification;
- fournir à l'organisme de surveillance applicable le rapport reçu aux termes du paragraphe 4.5.2, le cas échéant, et les commentaires reçus de cyberSanté Ontario ou du DRS qu'on soupçonne à l'origine des risques à la confidentialité ou à la sécurité ou qu'on soupçonne non conforme, selon le cas;
- fournir à l'organisme de surveillance applicable ses recommandations écrites.

4.5.5 En formulant ses recommandations à l'organisme de surveillance applicable aux termes du paragraphe 4.5.4, le comité de protection de la vie privée et de sécurité applicable doit faire ce qui suit :

- dans l'éventualité où il est recommandé d'effectuer une vérification, inclure des recommandations sur la nature et la portée de la vérification, la marche à suivre pour réaliser la vérification et le délai donné pour réaliser la vérification;
- dans l'éventualité où aucune vérification ne sera effectuée, inclure des recommandations, le cas échéant, sur les mesures proposées pour atténuer les risques à la confidentialité ou à la sécurité ou les éléments non conformes.

4.5.6 L'organisme de surveillance applicable doit, le plus tôt possible, mais, en toute circonstance, au plus tard à sa réunion suivant la réception de l'information et des recommandations demandées au paragraphe 4.5.4, faire ce qui suit :

- examiner l'information et les recommandations reçues;
- mettre une décision par écrit sur la pertinence pour le comité de protection de la vie privée et de sécurité applicable d'effectuer une vérification de cyberSanté Ontario ou du DRS qu'on soupçonne à l'origine des risques à la confidentialité ou à la sécurité ou qu'on soupçonne non conforme, selon le cas;
- dans l'éventualité où l'organisme de surveillance applicable a décidé qu'il fallait effectuer une vérification, fournir des directives écrites au comité de protection de la vie privée et de sécurité applicable, notamment la nature et la portée de la vérification, la marche à suivre pour réaliser la vérification et le délai donné pour réaliser la vérification;
- dans l'éventualité où l'organisme de surveillance applicable a décidé qu'il ne fallait pas effectuer de vérification, fournir des directives écrites, le cas échéant, au comité de protection de la vie privée et de sécurité applicable concernant les mesures proposées pour atténuer les risques à la confidentialité ou à la sécurité ou les éléments non conformes;
- fournir une copie de la décision et des directives au comité de protection de la vie privée et de sécurité applicable et à cyberSanté Ontario ou au DRS qu'on soupçonne à l'origine des risques à la confidentialité ou à la sécurité ou qu'on soupçonne non conforme, selon le cas.

4.5.7 Le comité de protection de la vie privée et de sécurité applicable doit effectuer une vérification conformément à la décision et aux directives de l'organisme de surveillance applicable.

4.5.8 cyberSanté Ontario ou le DRS qu'on soupçonne à l'origine des risques à la confidentialité ou à la sécurité ou qu'on soupçonne non conforme, selon le cas, doit se conformer à la décision et aux directives de l'organisme de surveillance applicable et doit atténuer les risques à la confidentialité ou à la sécurité ou les éléments non conformes ou coopérer dans tout exercice de vérification réalisé par le comité de protection de la vie privée et de sécurité applicable selon le cas.

4.5.9 Le comité de protection de la vie privée et de sécurité applicable doit, le plus tôt possible, mais, en toute circonstance, au plus tard à sa réunion suivant la fin de l'exercice de vérification, transmettre les éléments suivants à l'organisme de surveillance applicable :

- les résultats de la vérification;
- ses recommandations de mesures pour atténuer les risques à la confidentialité ou à la sécurité ou les éléments non conformes cernés, avec le délai donné pour mettre en œuvre les recommandations.

4.5.10 L'organisme de surveillance applicable doit, le plus tôt possible, mais, en toute circonstance, au plus tard à sa réunion suivant la réception de l'information et des recommandations demandées au paragraphe 4.5.9, faire ce qui suit :

- examiner l'information et les recommandations reçues;
- veiller à ce que tous les risques à la confidentialité et à la sécurité et les éléments non conformes aient été cernés;
- veiller à ce que les recommandations atténuent adéquatement les risques à la confidentialité et à la sécurité et les éléments non conformes cernés;
- mettre par écrit une décision visant à approuver les recommandations et fournir des directives concernant le délai à respecter pour mettre en œuvre la décision ou fournir des directives écrites au comité de protection de la vie privée et de sécurité applicable pour modifier les recommandations et

en présenter une version révisée et fournir le délai à respecter pour la modification et la présentation de la version révisée;

- fournir une copie de la décision et des directives au comité de protection de la vie privée et de sécurité applicable.

4.5.11 Le comité de protection de la vie privée et de sécurité applicable doit modifier les recommandations et en soumettre une version révisée à l'approbation de l'organisme de surveillance applicable dans le délai établi dans les directives écrites fournies aux termes du paragraphe 4.5.10 lorsqu'il reçoit la directive de le faire.

4.5.12 Le comité de protection de la vie privée et de sécurité applicable doit, à l'approbation des recommandations par l'organisme de surveillance applicable, fournir une copie des résultats de la vérification ainsi que de la décision et des directives de l'organisme de surveillance applicable à cyberSanté Ontario ou au DRS à l'origine des risques à la confidentialité ou à la sécurité ou non conforme.

4.5.13 cyberSanté Ontario ou le DRS à l'origine des risques à la confidentialité ou à la sécurité ou non conforme, selon le cas, doit, après la réception de l'information exigée au paragraphe 4.5.12, faire ce qui suit :

- mettre en œuvre la décision et les directives dans le délai approuvé par l'organisme de surveillance applicable;
- faire le point sur l'état de la mise en œuvre de la décision et des directives à chaque réunion du comité de protection de la vie privée et de sécurité applicable;
- fournir une mention écrite du comité de protection de la vie privée et de sécurité applicable attestant que la décision et les directives ont été entièrement mises en œuvre le plus tôt possible, mais, en toute circonstance, au plus tard trente (30) jours après la mise en œuvre.

4.5.14 Le comité de protection de la vie privée et de sécurité applicable doit surveiller la conformité de cyberSanté Ontario ou du DRS, selon le cas, à la mise en œuvre de la décision et des directives de l'organisme de surveillance applicable et peut exiger d'autres preuves de conformité. cyberSanté Ontario ou le DRS, selon le cas, doit se conformer à toute demande de preuves de conformité par le comité de protection de la vie privée et de sécurité applicable.

4.6 Non-conformité

4.6.1 Les cas de non-conformité à la LPRPS, aux ententes applicables ainsi qu'aux politiques, aux procédures et aux pratiques en vigueur concernant le DSE seront mis au jour par les activités suivantes décrites dans la présente politique :

- les ECVP;
- les auto-évaluations de la préparation en matière de confidentialité et de sécurité (le cas échéant);
- les auto-attestations opérationnelles en matière de confidentialité et de sécurité;
- la vérification de la conformité des mandataires, des fournisseurs de services électroniques et des tiers;
- les activités de vérification et de surveillance aux termes du paragraphe 4.5.1;
- les vérifications effectuées par le comité de protection de la vie privée et de sécurité applicable.

5 Application[4]

5.1.1 Tous les cas de non-respect seront examinés par le comité de protection de la vie privée et de sécurité applicable qui peut recommander la voie à suivre à l'organisme de surveillance applicable.

[4] Les références au comité de protection de la vie privée et de sécurité applicable et à l'organisme de surveillance applicable se trouvent au *Tableau 1 : Organismes administratifs applicables*.

5.1.2 L'organisme de surveillance applicable a le pouvoir d'imposer les sanctions appropriées, ce qui peut inclure la cessation des ententes applicables avec le DRS ou la cessation des privilèges d'accès des mandataires et des fournisseurs de services électroniques et une demande de mesures correctives.

6 Glossaire

Ententes applicables
Ententes conclues par les dépositaires de renseignements sur la santé, cyberSanté Ontario, les mandataires et les fournisseurs de services électroniques d'un DRS ou les mandataires et les fournisseurs de services électroniques de cyberSanté Ontario concernant le dossier de santé électronique.

Dossier de santé électronique (DSE)
Ensemble de la solution ConnexionOntario et du Dépôt des Services communs d'imagerie diagnostique, soit des dépôts ou des systèmes auxiliaires cliniques destinés à stocker et à rendre accessibles des renseignements personnels sur la santé contenus dans les systèmes électroniques de renseignements sur la santé des dépositaires de ces renseignements de manière à ne créer qu'un seul dépôt.

Organisme de surveillance applicable
Comité chargé d'approuver les stratégies, de faire connaître les risques à la confidentialité et à la sécurité et les éléments non conformes à son échelon supérieur ou de résoudre les situations ainsi problématiques, de prendre les décisions sur les objectifs stratégiques et les produits livrables à envisager et, selon le cas, d'approuver les recommandations du comité de protection de la vie privée et de sécurité applicable pour le dossier de santé électronique.

Comité de protection de la vie privée et de sécurité applicable
Comité prenant en charge la structure de gestion de la confidentialité et de la sécurité de l'information concernant le dossier de santé électronique et composé des dépositaires de renseignements sur la santé ou des mandataires de dépositaires de renseignements sur la santé qui créent et versent ou recueillent, utilisent ou divulguent des renseignements personnels sur la santé dans le dossier de santé électronique.

Fournisseur de services électroniques
Personne qui fournit des biens ou des services dans le but de permettre à un dépositaire de renseignements sur la santé d'employer des moyens électroniques de recueillir, d'utiliser, de modifier, de diffuser, de conserver ou d'éliminer des renseignements personnels sur la santé et qui comprend un fournisseur de réseau d'information sur la santé.

Haut placé
Terme pouvant englober le président du conseil d'administration ou le président, un vice-président, le secrétaire, le trésorier, le contrôleur, l'avocat général, le directeur général ou un directeur d'une société ou toute autre personne qui occupe un poste similaire à ceux habituellement occupés par les personnes nommées ci-dessus dans une société.

Structure d'administration de la politique	Solution ConnexionOntario	Dépôt des Services communs d'imagerie diagnostique
Comité de protection de la vie privée et de sécurité applicable	Protection de la vie privée : Comité de protection de la vie privée (Connecting Privacy) Sécurité : Comité de sécurité (Connecting Security)	Protection de la vie privée : Groupe de travail sur la protection de la vie privée et la sécurité des Services communs d'imagerie diagnostique Sécurité : Comité de sécurité (Connecting Security)
Organisme de surveillance applicable	Protection de la vie privée : Comité directeur de ConnexionOntario Sécurité : Comité stratégique de cyberSanté Ontario	Protection de la vie privée : Comité exécutif des Services communs d'imagerie diagnostique Sécurité : Comité stratégique de cyberSanté Ontario

Tableau 1 : Organismes administratifs applicables

Sigle	Terme
DRS	Dépositaire de renseignements sur la santé
RPS	Renseignements personnels sur la santé, tel que le terme est défini dans la *Loi de 2004 sur la protection des renseignements personnels sur la santé*
LPRPS	*Loi de 2004 sur la protection des renseignements personnels sur la santé*
ECVP	Évaluation des conséquences sur la vie privée
ERM	Évaluation des risques et des menaces

7 Références et documents connexes

- *Loi de 2004 sur la protection des renseignements personnels sur la santé* (LPRPS)
- *Politique de gestion de la confidentialité du dossier de santé électronique* et procédures connexes
- *Politique sur la journalisation et la vérification du dossier de santé électronique* et procédures connexes
- *Politique sur la journalisation et la surveillance du dossier de santé électronique* et procédures connexes
- *Politique de gestion des menaces et des risques relatifs au dossier de santé électronique* et procédures connexes

eHealth Ontario

Politique de gestion du consentement

Dossier de santé électronique

Version : 1.3

Nº de document : 3873

Ontario
eHealth Ontario

Gestion du document

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

Historique des approbations

APPROBATEURS	DATE D'APPROBATION
Membres du comité de protection de la vie privée ConnectingPrivacy	2014-04-30

Historique des révisions

NUMÉRO DE VERSION	DATE	RÉSUMÉ DES CHANGEMENTS	AUTEUR DES CHANGEMENTS
1.0	2014-11-17	Version définitive	Urooj Kirmani, analyste principal en protection de la vie privée, cyberSanté Ontario
0.01	2014-11-04	Première version établie en fonction de la politique harmonisée sur la gestion du consentement du comité de protection de la vie privée ConnectingPrivacy, v1.3	Promila Gonsalves, analyste en protection de la vie privée, cyberSanté Ontario

Table des matières

1 Objectif

Définir les politiques, les procédures et les pratiques qui s'appliquent à l'obtention du consentement d'une personne[1] concernant la collecte, l'utilisation ou la divulgation de ses renseignements personnels sur la santé (RPS) dans le dossier de santé électronique (DSE) afin qu'on prodigue ou contribue à prodiguer des soins de santé à cette personne.

Définir les politiques, les procédures et les pratiques qui s'appliquent à la mise en application de directives sur le consentement d'une personne en vue d'accorder, de refuser ou de retirer son consentement pour la collecte, l'utilisation ou la divulgation de ses RPS dans le DSE afin qu'on prodigue ou contribue à prodiguer des soins de santé à cette personne.

Définir les politiques, les procédures et les pratiques qui s'appliquent à la dérogation aux directives sur le consentement.

2 Portée

La présente politique et les procédures connexes s'appliquent à l'obtention d'un consentement, à la mise en application de directives sur le consentement ainsi qu'à la dérogation aux directives sur le consentement concernant les RPS d'une personne dans le DSE afin qu'on lui prodigue ou contribue à lui prodiguer des soins de santé et non à l'obtention d'un consentement, à la mise en application de directives sur le consentement ou à la dérogation aux directives sur le consentement pour tout autre RPS ou toute autre fin. Le DSE est composé de la solution ConnexionOntario et du Dépôt d'imagerie diagnostique des services hospitaliers. La solution ConnexionOntario et le Dépôt d'imagerie diagnostique des services hospitaliers sont des référentiels ou des systèmes auxiliaires cliniques destinés à stocker et à rendre accessibles des RPS contenus dans les systèmes électroniques de renseignements sur la santé des dépositaires de ces renseignements[2].

3 Politique

3.1 Fondements

3.1.1 La présente politique et les procédures connexes permettront aux dépositaires de renseignements sur la santé (DRS) et à cyberSanté Ontario de respecter les obligations que leur impose la *Loi de 2004 sur la protection des renseignements personnels sur la santé* (LPRPS) en ce qui concerne l'obtention du consentement; la réception et la mise en application de demandes de personnes visant à formuler, à modifier ou à retirer des directives sur le consentement ainsi qu'à la dérogation aux directives sur le consentement dans le DSE.

3.1.2 Les DRS et cyberSanté Ontario doivent avoir en place les politiques, les procédures et les pratiques sur la protection de la vie privée et la sécurité nécessaires pour les rendre conformes à leurs obligations aux termes de la LPRPS, des ententes applicables ainsi que de la présente politique et des procédures connexes.

---

[1] Le mot « personne » fait ici référence à la personne à qui appartiennent les RPS et comprend aussi le mandataire spécial de cette personne le cas échéant.

[2] Les divergences entre les exigences des politiques et des procédures de la solution ConnexionOntario et du référentiel du Service commun d'imagerie diagnostique sont indiquées dans la présente politique.

3.1.3 Les DRS et cyberSanté Ontario doivent prendre les mesures nécessaires et raisonnables selon les circonstances afin que leurs mandataires et leurs fournisseurs de services électroniques se conforment à la LPRPS, aux ententes applicables ainsi qu'à la présente politique et aux procédures connexes.

3.1.4 cyberSanté Ontario doit avoir un programme leur permettant, à lui et aux DRS, de remplir leurs obligations par rapport à la réception et à la mise en application de demandes de personnes visant à formuler, à modifier ou à retirer des directives sur le consentement ainsi que leurs obligations concernant la dérogation aux directives sur le consentement dans le DSE conformément à la LPRPS, aux ententes applicables ainsi qu'à la présente politique et aux procédures connexes.

3.1.5 Les DRS et cyberSanté Ontario doivent avoir en place des politiques, des procédures et des pratiques sur la protection de la vie privée et la sécurité qui respectent la LPRPS et informer leurs mandataires et leurs fournisseurs de services électroniques des politiques, des procédures et des pratiques imposées par la LPRPS.

Collecte, utilisation ou divulgation de RPS dans le DSE

3.1.6 En vertu du paragraphe 3.1.13, tout DRS a le droit de recueillir des RPS aux fins suivantes :

- prodiguer ou contribuer à prodiguer des soins de santé à la personne concernée;

Solution ConnexionOntario seulement

- éliminer ou réduire un risque important de lésion corporelle grave pour une personne ou un groupe de personnes lorsque le DRS est d'avis, selon des motifs raisonnables, que la collecte est nécessaire à une telle fin.

3.1.7 La LPRPS permet à un DRS de supposer le consentement implicite d'une personne de recueillir, d'utiliser ou de divulguer les RPS de cette dernière afin qu'on lui prodigue ou contribue à lui prodiguer des soins de santé, à moins que la personne ait expressément refusé ou retiré ce consentement.

3.1.8 Un DRS qui recueille les RPS du DSE d'une personne afin qu'on prodigue ou contribue à prodiguer des soins de santé à cette dernière peut utiliser ou divulguer les RPS à toutes les fins prévues par la LPRPS.

3.1.9 Un DRS qui recueille les RPS d'une personne ou d'un groupe de personnes dans la solution ConnexionOntario dans le but d'éliminer ou d'atténuer un risque important de lésion corporelle grave pour la personne ou le groupe de personnes ne pourra pas utiliser ni divulguer les RPS sauf aux fins auxquelles ces renseignements ont été recueillis.

Accorder, refuser ou retirer un consentement par des directives sur le consentement

3.1.10 La LPRPS donne le droit à une personne d'accorder, de refuser ou de retirer son consentement pour la collecte, l'utilisation ou la divulgation de ses RPS afin qu'on lui prodigue ou contribue à lui prodiguer des soins de santé. Cette personne peut exercer son droit en formulant, en modifiant ou en retirant une directive sur le consentement.

3.1.11 La personne peut formuler, modifier ou retirer les directives sur le consentement suivantes concernant ses RPS dans le DSE :

Dépôt d'imagerie diagnostique des services hospitaliers[3]:

- directives sur le consentement pour référentiels;
- directives sur le consentement pour dossiers de DRS[4];

Solution ConnexionOntario:

- directives sur le consentement global[5];

[3] Des fonctionnalités de gestion du consentement seront ajoutées au fur et à mesure que la technologie le permettra.

[4] La directive sur le consentement pour dossiers de DRS ne s'applique pas pour le moment. Les DRS seront avisés lorsque la fonctionnalité sera active.

[5] La directive sur le consentement global et la directive sur le consentement pour référentiels constituent actuellement la même chose étant donné que le DSE est le seul référentiel visé par la *Politique sur la gestion du consentement relative au dossier de santé électronique* et les procédures connexes, ce qui comprend les modifications qui y sont apportées de temps à autre.

- directives sur le consentement pour référentiels;
- directives sur le consentement pour dossiers de DRS;
- directives sur le consentement pour mandataires de DRS;
- directives sur le consentement pour mandataires.

3.1.12 La présente politique et les procédures connexes aideront toute personne à exercer son droit d'accorder, de refuser ou de retirer son consentement pour la collecte, l'utilisation ou la divulgation de ses RPS dans le DSE afin qu'on lui prodigue ou contribue à lui prodiguer des soins de santé.

Dérogation aux directives sur le consentement

3.1.13 Un DRS ou un mandataire de DRS ne peut déroger à une directive sur le consentement concernant la collecte de RPS que dans les cas suivants :

- le DRS ou le mandataire du DRS obtient le consentement exprès de la personne que concernent les RPS;

Solution ConnexionOntario seulement

- le DRS ou le mandataire du DRS a des motifs raisonnables de croire que la collecte est nécessaire dans le but d'éliminer ou d'atténuer un risque important de lésion corporelle grave pour la personne que concernent les RPS et qu'il n'est pas possible, dans la mesure du raisonnable, d'obtenir le consentement de la personne à temps;
- le DRS ou le mandataire du DRS a des motifs raisonnables de croire que la collecte est nécessaire dans le but d'éliminer ou d'atténuer un risque important de lésion corporelle grave pour une personne autre que la personne que concernent les RPS ou un groupe de personnes.

3.1.14 Un DRS ou un mandataire de DRS qui déroge à une directive sur le consentement pour la collecte de RPS dans le DSE ne doit utiliser ou divulguer ces RPS qu'aux fins auxquelles ils ont été recueillis.

3.1.15 Tous les cas dans lesquels on déroge à une directive sur le consentement pour recueillir les RPS dans le DSE en partie ou en totalité doivent faire l'objet d'une vérification et d'une surveillance, et un avis de la collecte des renseignements doit être fourni au DRS ou au DRS dont les mandataires ont recueilli les RPS visés par la directive sur le consentement ainsi qu'à la personne que concernent les RPS.

4 Procédures

4.1 Procédures pour obtenir un consentement

4.1.1 Les DRS doivent obtenir le consentement d'une personne avant d'en recueillir, utiliser et divulguer les RPS contenus dans le DSE conformément à la LPRPS ainsi qu'à leurs politiques, à leurs procédures et à leurs pratiques internes.

4.1.2 Les DRS doivent afficher, rendre accessible sur-le-champ ou fournir l'avis décrit au paragraphe 4.1.3 pour les personnes concernées.

4.1.3 cyberSanté Ontario doit rendre un avis accessible aux DRS qui contient les éléments suivants :

- une description générale des RPS dans le DSE;
- une description des mesures de protection administratives, techniques et matérielles pour les RPS contenus dans le DSE ainsi que les pratiques adoptées à leur égard;
- une description des personnes et des organisations ayant la permission de recueillir, d'utiliser et de divulguer les RPS dans le DSE;
- une description des raisons pour lesquelles ces personnes et ces organisations peuvent recueillir, utiliser et divulguer les RPS dans le DSE;
- une mention selon laquelle les personnes concernées ont le droit d'accorder, de refuser ou de retirer leur consentement pour la collecte, l'utilisation ou la divulgation de leurs RPS dans le DSE afin qu'on leur prodigue ou contribue à leur prodiguer des soins de santé en formulant, en modifiant ou en retirant des directives sur le consentement;

- une indication des coordonnées des personnes-ressources à qui les personnes concernées peuvent transmettre leur demande de formuler, de modifier ou de retirer des directives sur le consentement dans le DSE;
- une indication des coordonnées des personnes-ressources à qui les personnes concernées peuvent transmettre leur demande d'accéder à leurs RPS dans le DSE ou de corriger les RPS et poser des questions ou déposer des plaintes concernant leurs RPS dans le DSE;
- une description de la marche à suivre pour faire une plainte au commissaire à l'information et à la protection de la vie privée de l'Ontario concernant le DSE.

4.2 Procédures pour recevoir et mettre en application des directives sur le consentement

Réception des directives sur le consentement

4.2.1 Lorsqu'un DRS ou cyberSanté Ontario reçoit une demande de formulation, de modification ou de retrait d'une directive sur le consentement dans le DSE, le DRS ou cyberSanté Ontario devra répondre à la demande conformément à ses politiques, à ses procédures et à ses pratiques internes ainsi qu'aux exigences du paragraphe 4.2.2.

4.2.2 À la réception d'une demande de la part d'une personne de formuler, de modifier ou de retirer une directive sur le consentement dans le DSE, cyberSanté Ontario ou le DRS doit faire ce qui suit :

- journaliser la réception de la demande;
- vérifier si la personne qui fait la demande est bel et bien la personne que concernent les RPS faisant l'objet de la demande ou son mandataire spécial;
- obtenir de la personne assez de renseignements pour identifier la personne dans le DSE, trouver ses RPS dans le DSE et donner suite à la demande;
- si la demande ne contient pas assez de renseignements, offrir de l'aide au demandeur;
- informer la personne des conséquences de la formulation, de la modification ou du retrait d'une directive sur le consentement;
- informer la personne des circonstances dans lesquelles il est possible de déroger à une directive sur le consentement pour recueillir des RPS;
- informer la personne du fait qu'elle recevra un avis dans tous les cas où une partie ou la totalité de ses RPS dans le DSE est recueillie parce qu'on a pu déroger à une directive sur le consentement;
- informer la personne du fait qu'elle peut formuler, modifier ou retirer une directive sur le consentement en tout temps;
- obtenir auprès de la personne une adresse pour l'envoi de l'avis exigé aux termes du paragraphe 4.4.1;
- le cas échéant, aviser la personne du fait que la demande sera transmise à cyberSanté Ontario pour qu'on puisse y donner suite.

4.2.3 Les paragraphes 4.2.1 et 4.2.2 ne s'appliquent pas lorsqu'un DRS reçoit une demande de formulation, de modification ou de retrait d'une directive sur le consentement pour dossiers de DRS concernant des RPS qui ont été créés et versés dans le DSE par un autre DRS.

4.2.4 À la demande de cyberSanté Ontario, les DRS doivent aider cyberSanté Ontario à vérifier si la personne qui fait la demande est bel et bien la personne que concernent les RPS faisant l'objet de la demande ou son mandataire spécial.

Mise en application des directives sur le consentement global, pour référentiels et pour mandataires de DRS (le cas échéant)

4.2.5 Lorsqu'un DRS ou cyberSanté Ontario reçoit une demande d'une personne qui désire formuler, modifier ou retirer une directive sur le consentement global, une directive sur le consentement pour référentiels ou une directive sur le consentement pour mandataires de DRS (selon le cas conformément au paragraphe 3.1.11) dans le DSE, le DRS ou cyberSanté Ontario doit, le plus tôt possible, mais, en toute circonstance, au plus tard sept (7) jours après la vérification de l'identité du demandeur, faire ce qui suit :

- donner suite à la demande;

- prendre toutes les mesures raisonnables pour confirmer qu'on a donné suite à la demande.

4.2.6 Tout de suite après avoir donné suite à la demande et pris toutes les mesures raisonnables pour confirmer qu'on a donné suite à la demande, le DRS qui a reçu la demande ou cyberSanté Ontario, si elle a reçu la demande, doit fournir à la personne l'avis exigé au paragraphe 4.4.1.

Mise en application de directives sur le consentement pour dossiers de DRS[6]

4.2.7 Lorsqu'un DRS reçoit une demande d'une personne qui désire formuler, modifier ou retirer une directive sur le consentement pour dossiers de DRS concernant ses RPS créés ou versés dans le DSE, le DRS doit faire ce qui suit :

- donner suite à la demande et prendre toutes les mesures raisonnables pour confirmer qu'on a donné suite à la demande le plus tôt possible, mais, en toute circonstance, au plus tard sept (7) jours après la vérification de l'identité du demandeur;
- tout de suite après avoir donné suite à la demande et pris toutes les mesures raisonnables pour confirmer qu'on a donné suite à la demande, fournir à la personne l'avis exigé au paragraphe 4.4.1.

4.2.8 Lorsque le DRS n'est pas en mesure de donner suite à la demande aux termes du paragraphe 4.2.7 directement dans le DSE, il doit transmettre la demande à cyberSanté Ontario le plus tôt possible, mais, en toute circonstance, au plus tard sept (7) jours après la vérification de l'identité du demandeur.

4.2.9 Lorsqu'il transmet une demande à cyberSanté Ontario aux termes du paragraphe 4.2.8, le DRS doit inclure les éléments suivants :

- l'identité de la personne que concernent les RPS faisant l'objet de la demande;
- la demande de la personne qui désire formuler, modifier ou retirer une directive sur le consentement pour dossiers de DRS;
- assez de renseignements pour identifier la personne dans le DSE, trouver les RPS de la personne dans le DSE, identifier le DRS faisant l'objet de la demande et donner suite à la demande.

4.2.10 À la réception d'une demande transmise aux termes du paragraphe 4.2.8, cyberSanté Ontario doit donner suite à la demande et prendre toutes les mesures raisonnables pour confirmer qu'on a donné suite à la demande le plus tôt possible, mais, en toute circonstance, au plus tard sept (7) jours après la réception des renseignements dont il est question au paragraphe 4.2.9.

4.2.11 cyberSanté Ontario doit, le plus tôt possible après avoir donné suite à la demande et avoir pris toutes les mesures raisonnables pour confirmer qu'on a donné suite à la demande conformément au paragraphe 4.2.10, informer le DRS qu'on a donné suite à la demande, qu'on a confirmé la chose et que le DRS doit fournir à la personne l'avis exigé au paragraphe 4.4.1.

4.2.12 Tout de suite après avoir reçu l'avis aux termes du paragraphe 4.2.11, le DRS doit fournir à la personne l'avis exigé au paragraphe 4.4.1.

4.2.13 Lorsqu'un DRS reçoit une demande pour formuler, modifier ou retirer une directive sur le consentement pour dossiers de DRS concernant les RPS créés et versés dans le DSE par un autre DRS, le DRS qui reçoit la demande doit, le plus tôt possible, mais, en toute circonstance, au plus tard sept (7) jours après la réception de la demande, faire ce qui suit :

- aviser la personne du fait que le DRS n'est pas en mesure de donner suite à la demande parce qu'elle concerne des RPS créés et versés dans le DSE par un autre DRS;
- fournir à la personne l'information lui permettant de communiquer avec cyberSanté Ontario pour qu'on mette en application la directive sur le consentement.

4.2.14 Lorsque cyberSanté Ontario reçoit une demande d'une personne qui désire formuler, modifier ou retirer une directive sur le consentement pour dossiers de DRS concernant ses RPS dans le DSE, cyberSanté Ontario doit faire ce qui suit :

---

[6] La directive sur le consentement pour dossiers de DRS ne s'applique actuellement pas pour le Service commun d'imagerie diagnostique. Les DRS seront avisés lorsque la fonctionnalité sera active.

- donner suite à la demande et prendre toutes les mesures raisonnables pour confirmer qu'on a donné suite à la demande le plus tôt possible, mais, en toute circonstance, au plus tard sept (7) jours après la vérification de l'identité du demandeur;
- à la demande de la personne, aviser le DRS qui a créé et versé les RPS qui font l'objet de la directive sur le consentement pour dossiers de DRS du fait qu'une directive sur le consentement pour dossiers de DRS a été formulée, modifiée ou retirée;
- tout de suite après avoir donné suite à la demande et pris toutes les mesures raisonnables pour confirmer qu'on a donné suite à la demande, fournir à la personne l'avis exigé au paragraphe 4.4.1.

Mise en application de directives sur le consentement pour mandataires (le cas échéant)

4.2.15 Lorsqu'un DRS ou reçoit une demande d'une personne qui désire formuler, modifier ou retirer une directive sur le consentement pour mandataires (selon le cas conformément au paragraphe 3.1.11) dans le DSE, le DRS doit, le plus tôt possible, mais, en toute circonstance, au plus tard sept (7) jours après la vérification de l'identité du demandeur, faire ce qui suit :

- donner suite à la demande et prendre toutes les mesures raisonnables pour confirmer qu'on a donné suite à la demande;
- transmettre la demande à cyberSanté Ontario.

4.2.16 Lorsqu'il transmet une demande à cyberSanté Ontario aux termes du paragraphe 4.2.15, le DRS doit inclure les éléments suivants :

- l'identité de la personne que concernent les RPS faisant l'objet de la demande;
- la demande de la personne qui désire formuler, modifier ou retirer une directive sur le consentement pour mandataires;
- la directive sur le consentement pour mandataires appliquée par le DRS;
- assez de renseignements pour identifier la personne dans le DSE, trouver les RPS de la personne dans le DSE, identifier le mandataire ou les mandataires faisant l'objet de la demande et donner suite à la demande.

4.2.17 À la réception d'une demande transmise aux termes du paragraphe 4.2.15, cyberSanté Ontario doit, le plus tôt possible, mais, en toute circonstance, au plus tard sept (7) jours après la réception de l'information conformément au paragraphe 4.2.16, faire ce qui suit :

- prendre toutes les mesures raisonnables pour identifier tous les DRS au nom desquels le mandataire ou les mandataires faisant l'objet de la demande recueillent, utilisent ou divulguent les RPS dans le DSE;
- donner suite à la demande et prendre toutes les mesures raisonnables pour confirmer qu'on a donné suite à la demande, peu importe qui sont les DRS au nom desquels le mandataire ou les mandataires recueillent, utilisent ou divulguent les RPS dans le DSE;
- aviser le DRS du fait qu'on a donné suite à la demande, qu'on a confirmé la chose et que le DRS doit fournir à la personne l'avis exigé aux termes du paragraphe 4.4.1.

4.2.18 Tout de suite après avoir reçu l'avis aux termes du paragraphe 4.2.17, le DRS doit fournir à la personne l'avis exigé au paragraphe 4.4.1.

4.2.19 Lorsque cyberSanté Ontario ou reçoit une demande d'une personne qui désire formuler, modifier ou retirer une directive sur le consentement pour mandataires dans le DSE, cyberSanté Ontario doit, le plus tôt possible, mais, en toute circonstance, au plus tard sept (7) jours après la vérification de l'identité du demandeur, faire ce qui suit :

- prendre toutes les mesures raisonnables pour identifier tous les DRS au nom desquels le mandataire ou les mandataires faisant l'objet de la demande recueillent, utilisent ou divulguent les RPS dans le DSE;
- donner suite à la demande et prendre toutes les mesures raisonnables pour confirmer qu'on a donné suite à la demande, peu importe qui sont les DRS au nom desquels le mandataire ou les mandataires recueillent, utilisent ou divulguent les RPS dans le DSE.

4.2.20 Tout de suite après avoir donné suite à la demande et pris toutes les mesures raisonnables pour confirmer qu'on a donné suite à la demande aux termes du paragraphe 4.2.19, cyberSanté Ontario doit fournir à la personne l'avis exigé au paragraphe 4.4.1.

4.2.21 En prenant toutes les mesures raisonnables pour identifier tous les DRS au nom desquels le mandataire ou les mandataires faisant l'objet de la demande recueillent, utilisent et divulguent les RPS dans le DSE ainsi qu'en prenant toutes les mesures raisonnables pour donner suite à la demande, peu importe qui sont les DRS au nom desquels le mandataire ou les mandataires recueillent, utilisent ou divulguent les RPS dans le DSE, cyberSanté Ontario doit faire ce qui suit :

- faire une recherche dans le dépôt du fournisseur pour trouver tous les comptes potentiels associés au mandataire ou aux mandataires faisant l'objet de la demande;
- communiquer avec le mandataire ou les mandataires faisant l'objet de la demande pour trouver et confirmer tout autre DRS au nom duquel le mandataire ou les mandataires recueillent, utilisent ou divulguent les RPS dans le DSE;
- communiquer avec chaque DRS pour vérifier si le mandataire ou les mandataires recueillent, utilisent ou divulguent les RPS au nom du DRS et vérifient si le compte dans le dépôt du fournisseur est associé au mandataire ou aux mandataires faisant l'objet de la demande;
- mettre en application une directive sur le consentement pour mandataires pour chaque compte potentiel associé au mandataire ou aux mandataires faisant l'objet de la demande.

4.2.22 Après avoir mis en application une directive sur le consentement pour mandataires et pris toutes les mesures raisonnables pour confirmer qu'une telle directive a été mise en application aux termes des paragraphes 4.2.17 ou 4.2.19, selon le cas, cyberSanté Ontario doit assurer une vérification et une surveillance constantes de la directive sur le consentement pour mandataires pour veiller à ce qu'elle continue de s'appliquer à tous les mandataires faisant l'objet de la directive, peu importe les DRS au nom desquels le mandataire ou les mandataires recueillent, utilisent ou divulguent les RPS dans le DSE.

4.2.23 Pour assurer une vérification et une surveillance constantes des directives sur le consentement pour mandataires aux termes du paragraphe 4.2.22, cyberSanté Ontario doit faire ce qui suit :

- conserver une liste de tous les mandataires faisant l'objet d'une directive sur le consentement pour mandataires;
- surveiller les changements apportés aux comptes associés aux mandataires faisant partie de la liste des mandataires faisant l'objet d'une directive sur le consentement pour mandataires;
- évaluer les changements apportés aux comptes des mandataires et réviser la directive sur le consentement pour mandataires selon les besoins.

4.3 Procédures pour mettre à l'essai et confirmer les directives sur le consentement mises en application

4.3.1 Les DRS et cyberSanté Ontario doivent prendre toutes les mesures raisonnables pour confirmer que les qu'on donne adéquatement suite aux demandes pour formuler, modifier ou retirer les directives sur le consentement qu'ils ont mises en application dans le DSE.

4.4 Procédures pour aviser les personnes de la mise en application d'une directive sur le consentement

4.4.1 Tout de suite après que le DRS ayant reçu une demande d'une personne qui désire formuler, modifier ou retirer une directive sur le consentement ou que cyberSanté Ontario, s'il a reçu une telle demande, a donné suite à la demande et a pris toutes les mesures raisonnables pour confirmer qu'on a donné suite à la demande dans le DSE ou a reçu l'avis selon lequel on a donné suite à la demande et que la chose a été confirmée dans le DSE, selon le cas, le DRS ou cyberSanté Ontario doit fournir à la personne un avis contenant les éléments suivants :

- une description de la demande reçue de la personne;
- une identification et une description de la directive sur le consentement qui a été formulée, modifiée ou retirée dans le DSE;
- une confirmation selon laquelle la directive sur le consentement a été formulée, modifiée ou retirée et la date à laquelle a eu lieu la formulation, la modification ou le retrait;
- une description des conséquences de la formulation, de la modification ou du retrait de la directive sur le consentement;

- une description des circonstances dans lesquelles il est possible de déroger à la directive sur le consentement pour recueillir des RPS;
- une indication selon laquelle la personne recevra un avis dans tous les cas où une partie ou la totalité de ses RPS dans le DSE est recueillie parce qu'on a pu déroger à une directive sur le consentement;
- les coordonnées de la personne-ressource à qui il est possible de poser des questions ou de formuler une plainte concernant la directive sur le consentement;
- une indication selon laquelle la personne peut formuler, modifier ou retirer une directive sur le consentement en tout temps;
- lorsque cyberSanté Ontario fournit l'avis, une indication selon laquelle cyberSanté Ontario fournit l'avis au nom des DRS qui recueillent, utilisent ou divulguent les RPS dans le DSE.

4.4.2 Le DRS ou cyberSanté Ontario, selon le cas, doit conserver une copie de l'avis fourni à la personne aux termes du paragraphe 4.4.1 ou un journal des avis fournis.

4.5 Procédures pour journaliser, vérifier et surveiller les directives sur le consentement formulées, modifiées ou retirées

4.5.1 cyberSanté Ontario doit veiller à ce que le DSE puisse garder un journal de tous les cas où une directive sur le consentement est formulée, modifiée ou retirée dans le DSE et à ce que le journal contienne l'information exigée par la LPRPS et la *Politique pour la journalisation et la vérification du dossier de santé électronique* et les procédures connexes, ce qui comprend les modifications qui y sont apportées de temps à autre.

4.5.2 cyberSanté Ontario doit vérifier et surveiller tous les cas où une directive sur le consentement est formulée, modifiée ou retirée dans le DSE conformément à la *Politique pour la journalisation et la vérification du dossier de santé électronique* et aux procédures connexes, ce qui comprend les modifications qui y sont apportées de temps à autre.

4.5.3 Les DRS doivent vérifier et surveiller tous les cas où le DRS et les mandataires ou les fournisseurs de services électroniques du DRS, autres que cyberSanté Ontario et les mandataires ou les fournisseurs de services électroniques de cyberSanté Ontario, ont donné suite à la demande d'une personne qui désire formuler, modifier ou retirer une directive sur le consentement dans le DSE conformément à la *Politique pour la journalisation et la vérification du dossier de santé électronique* et aux procédures connexes, ce qui comprend les modifications qui y sont apportées de temps à autre.

4.6 Procédures pour déroger à une directive sur le consentement

4.6.1 cyberSanté Ontario doit veiller à ce que le DSE soit en mesure d'aviser le DRS ou le mandataire du DRS si les RPS qu'on tente de recueillir font l'objet d'une directive sur le consentement sans fournir de RPS faisant l'objet de la directive sur le consentement.

4.6.1.1 cyberSanté Ontario doit veiller à ce que le DSE exige du DRS ou du mandataire du DRS qui cherche à recueillir les RPS faisant l'objet d'une directive sur le consentement qu'il identifie les motifs, parmi les trois permis, pour lesquels on déroge à la directive sur le consentement dans le but de recueillir les RPS, en particulier si le DSR ou le mandataire du DSR qui cherche à recueillir les RPS respecte les conditions suivantes :

- il a obtenu le consentement exprès de la personne que concernent les RPS;

Solution ConnexionOntario seulement

- il a des motifs raisonnables de croire que la collecte est nécessaire dans le but d'éliminer ou d'atténuer un important risque de lésion corporelle grave pour la personne que concernent les RPS et qu'il n'est pas possible, dans la mesure du raisonnable, d'obtenir le consentement de la personne à temps;
- il a des motifs raisonnables de croire que la collecte est nécessaire dans le but d'éliminer ou d'atténuer un important risque de lésion corporelle grave pour une personne autre que la personne que concernent les RPS ou un groupe de personnes.

4.6.2 Le DRS ou le mandataire du DRS qui cherche à recueillir les RPS dans le DSE faisant l'objet d'une directive sur le consentement doit indiquer la raison pour laquelle, aux termes du paragraphe 4.6.1.1, on déroge à la directive sur le consentement pour recueillir les RPS.

4.6.3 Le DRS ou le mandataire du DRS qui cherche à recueillir les RPS dans le DSE faisant l'objet d'une directive sur le consentement à la suite du consentement exprès de la personne doit obtenir ledit consentement conformément à la LPRPS; aux politiques, aux procédures et aux pratiques internes du DRS ainsi qu'aux exigences du paragraphe 4.6.4.

4.6.4 En vue d'obtenir le consentement exprès de la personne, le DRS ou le mandataire du DRS qui cherche à recueillir les RPS dans le DSE faisant l'objet d'une directive sur le consentement doit veiller à ce que la personne connaisse l'information suivante :

- le but de la collecte;
- la possibilité qu'elle a d'accorder ou de refuser son consentement;
- le fait qu'on ne dérogera à la directive sur le consentement que pour une durée de quatre (4) heures pour le Dépôt d'imagerie diagnostique des services hospitaliers et de vingt-quatre (24) heures pour la solution ConnexionOntario;
- le fait que les RPS ne seront utilisés ou divulgués qu'aux fins auxquelles ils ont été recueillis.

4.6.5 cyberSanté Ontario doit veiller à ce que le DSE soit en mesure de créer un journal pour tous les cas dans lesquels une partie ou la totalité des RPS dans le DSE est divulguée à un DRS ou recueillie par un DRS ou un mandataire de DRS qui a pu déroger à une directive sur le consentement.

4.6.6 cyberSanté Ontario doit veiller à ce que le journal de tous les cas où une partie ou la totalité des RPS dans le DSE est divulguée à un DRS ou à un mandataire de DRS qui a pu déroger à une directive sur le consentement contienne les renseignements exigés par la LPRPS et la *Politique pour la journalisation et la vérification du dossier de santé électronique* et les procédures connexes, ce qui comprend les modifications qui y sont apportées de temps à autre.

4.6.7 cyberSanté Ontario doit assurer la vérification et la surveillance constantes du journal exigé au paragraphe 4.6.6 conformément à la *Politique pour la journalisation et la vérification du dossier de santé électronique* et aux procédures connexes, ce qui comprend les modifications qui y sont apportées de temps à autre, et fournir sur-le-champ un avis écrit au DRS ou au DRS dont le mandataire a dérogé à une directive sur le consentement dans le DSE pour recueillir les RPS. L'avis doit au minimum inclure les éléments suivants :

- le DRS qui a divulgué les RPS faisant l'objet de la directive sur le consentement;
- le DRS qui a recueilli les RPS faisant l'objet de la directive sur le consentement;
- le mandataire du DRS qui a recueilli les RPS faisant l'objet de la directive sur le consentement;

- la personne que concernent les RPS faisant l'objet de la directive sur le consentement;
- le type de RPS faisant l'objet de la directive sur le consentement qui ont été recueillis;
- la date et l'heure auxquelles les RPS faisant l'objet de la directive sur le consentement ont été recueillis;
- la raison pour laquelle on a dérogé à la directive sur le consentement pour recueillir les RPS.

4.6.8 À la réception de l'avis exigé au paragraphe 4.6.7, le DRS qui a dérogé ou dont le mandataire a dérogé à une directive sur le consentement dans le DSE pour recueillir les RPS doit, à la première occasion possible, fournir un avis à la personne que concernent les RPS. L'avis doit être écrit ou dans la forme demandée par la personne. L'avis doit au minimum indiquer qu'on a dérogé à une directive sur le consentement pour recueillir ses RPS et contenir les éléments suivants :

- le type de RPS faisant l'objet de la directive sur le consentement qui ont été recueillis;
- le DRS qui a recueilli les RPS faisant l'objet de la directive sur le consentement;
- le mandataire du DRS qui a recueilli les RPS faisant l'objet de la directive sur le consentement;
- la date et l'heure auxquelles les RPS faisant l'objet de la directive sur le consentement ont été recueillis;
- le DRS qui a divulgué les RPS faisant l'objet de la directive sur le consentement;
- la raison pour laquelle on a dérogé à la directive sur le consentement pour recueillir les RPS;
- la personne-ressource à qui la personne peut poser des questions ou formuler des plaintes sur le fait qu'on a dérogé à une directive sur le consentement ainsi que les coordonnées de cette personne-ressource;
- la démarche à suivre pour déposer une plainte auprès du commissaire à l'information et à la protection de la vie privée de l'Ontario.

4.6.9 Un DRS qui a dérogé ou dont le mandataire a dérogé à une directive sur le consentement dans le DSE pour recueillir les RSP doit garder une copie de l'avis fourni à la personne aux termes du paragraphe 4.6.8 ou un journal des avis fournis.

Procédures supplémentaires pour déroger à une directive sur le consentement dans le cas de la solution ConnexionOntario

4.6.10 Un DRS qui a dérogé ou dont le mandataire a dérogé à une directive sur le consentement dans le DSE pour recueillir les RPS dans le but d'éliminer ou d'atténuer un risque important de lésion corporelle grave pour une personne autre que la personne que concernent les RPS ou un groupe de personnes ne doit pas fournir de renseignements qui identifient la personne ou le groupe de personnes présentant un risque important de lésion corporelle grave dans l'avis exigé au paragraphe 4.6.8.

4.6.11 Un DRS qui a dérogé ou dont le mandataire a dérogé à une directive sur le consentement dans le DSE pour recueillir les RPS dans le but d'éliminer ou d'atténuer un risque important de lésion corporelle grave pour une personne autre que la personne que concernent les RPS ou un groupe de personnes doit fournir un avis écrit au commissaire à l'information et à la protection de la vie privée de l'Ontario d'une manière qui ne fournit pas de renseignements qui identifie la personne que concernent les RPS ou la personne ou le groupe de personnes présentant un risque important de lésion corporelle grave.

4.6.12 L'avis exigé aux termes du paragraphe 4.6.11 doit être fourni au commissaire à l'information et à la protection de la vie privée de l'Ontario le plus tôt possible, mais, en toute circonstance, au plus tard sept (7) jours après la réception de l'avis exigé au paragraphe 4.6.7 et doit contenir les éléments suivants :

- le DRS qui a divulgué les RPS faisant l'objet de la directive sur le consentement;
- le DRS qui a recueilli les RPS faisant l'objet de la directive sur le consentement;
- le mandataire du DRS qui a recueilli les RPS faisant l'objet de la directive sur le consentement;
- le type de RPS faisant l'objet de la directive sur le consentement qui ont été recueillis;
- la date et l'heure auxquelles les RPS faisant l'objet de la directive sur le consentement ont été recueillis.

5 Application[7]

5.1.1 Tous les cas de non-respect seront examinés par le comité de protection de la vie privée et de sécurité applicable qui recommandera la voie à suivre à l'organisme de surveillance applicable.

5.1.2 L'organisme de surveillance applicable a le pouvoir d'imposer les sanctions appropriées, ce qui peut inclure la cessation des ententes applicables avec le DRS ou la cessation des privilèges d'accès des mandataires et des fournisseurs de services électroniques et une demande de mesures correctives.

6 Glossaire

Dossier de santé électronique (DSE)
Ensemble de la solution ConnexionOntario et du Dépôt d'imagerie diagnostique des services hospitaliers, soit des dépôts ou des systèmes auxiliaires cliniques destinés à stocker et à rendre accessibles des renseignements personnels sur la santé contenus dans les systèmes électroniques de renseignements sur la santé des dépositaires de ces renseignements de manière à ne créer qu'un seul dépôt.

Directive sur le consentement pour mandataires
Directive sur le consentement formulée par une personne en vue d'accorder, de refuser ou de retirer son consentement à la collecte, à l'utilisation et à la divulgation de tous ses renseignements personnels sur la santé dans le dossier de santé électronique par un mandataire ou plus d'un mandataire, mais pas la totalité d'entre eux, d'un dépositaire de renseignements sur la santé ou de plus d'un dépositaire de renseignements sur la santé, mais pas la totalité d'entre eux.

Directive sur le consentement
Directive formulée par une personne en vue de refuser ou de retirer, en partie ou en totalité, son consentement à la collecte, à l'utilisation ou à la divulgation de ses renseignements personnels sur la santé dans le dossier de santé électronique dans le but de lui prodiguer ou de contribuer à lui prodiguer des soins de santé, directive qui comprend la possibilité de modifier ou de supprimer une directive qui a déjà été présentée.

Les renseignements suivants ne peuvent pas faire l'objet d'une directive sur le consentement parce qu'ils sont nécessaires pour identifier la personne dans le dossier de santé électronique, ce qui assure le respect des procédures relatives à la vie privée de la personne ainsi que l'exactitude des renseignements personnels sur la santé dans le dossier de santé électronique :

- le prénom;
- le nom;
- le sexe;
- la date de naissance;
- l'adresse principale (rue, code postal, ville, province, pays);
- le numéro de la carte d'assurance maladie (le cas échéant);
- le numéro du dépositaire de renseignements sur la santé et le numéro de dossier médical attribué par le dépositaire (le cas échéant).

Directive sur le consentement pour dépôts
Directive sur le consentement formulée par une personne en vue de refuser ou de retirer son consentement à la collecte, à l'utilisation et à la divulgation de tous ses renseignements personnels sur la santé dans un dépôt ou plus d'un dépôt, mais pas la totalité d'entre eux, dans [NOM DU SYSTÈME][8].

---

[7] Les références au comité de protection de la vie privée et de sécurité applicable et à l'organisme de surveillance applicable se trouvent au *Tableau 1 : Organismes administratifs applicables*.

[8] La directive sur le consentement global et la directive sur le consentement pour dépôts constituent actuellement la même chose étant donné que le dossier de santé électronique est le seul dépôt visé par la *Politique sur la gestion du consentement relative au dossier de santé électronique* et aux procédures connexes, ce qui comprend les modifications qui y sont apportées de temps à autre.

Fournisseur de services électroniques
Personne qui fournit des biens ou des services dans le but de permettre à un dépositaire de renseignements sur la santé d'employer des moyens électroniques de recueillir, d'utiliser, de modifier, de diffuser, de conserver ou d'éliminer des renseignements personnels sur la santé et qui comprend un fournisseur de réseau d'information sur la santé.

Directive sur le consentement global
Directive sur le consentement formulée par une personne en vue de refuser ou de retirer son consentement à la collecte, à l'utilisation et à la divulgation de tous ses renseignements personnels sur la santé dans le dossier de santé électronique[9].

Directive sur le consentement pour mandataires de DRS
Directive sur le consentement formulée par une personne en vue d'accorder, de refuser ou de retirer son consentement à la collecte, à l'utilisation et à la divulgation de tous ses renseignements personnels sur la santé dans le dossier de santé électronique par tous les mandataires d'un dépositaire de renseignements sur la santé ou de plus d'un dépositaire de renseignements sur la santé, mais pas la totalité d'entre eux.

Directive sur le consentement pour dossiers de DRS
Directive sur le consentement formulée par une personne en vue d'accorder, de refuser ou de retirer son consentement à la collecte, à l'utilisation et à la divulgation de tous les renseignements personnels sur la santé créés et versés dans le dossier de santé électronique par un dépositaire de renseignements sur la santé ou plus d'un dépositaire de renseignements sur la santé, mais pas la totalité d'entre eux.

Structure d'administration de la politique	Solution ConnexionOntario	Dépôt des Services communs d'imagerie diagnostique
Comité de protection de la vie privée et de sécurité applicable	Protection de la vie privée : Comité de protection de la vie privée (Connecting Privacy) Sécurité : Comité de sécurité (Connecting Security)	Protection de la vie privée : Groupe de travail sur la protection de la vie privée et la sécurité des Services communs d'imagerie diagnostique Sécurité : Comité de sécurité (Connecting Security)
Organisme de surveillance applicable	Protection de la vie privée : Comité directeur de ConnexionOntario Sécurité : Comité stratégique de cyberSanté Ontario	Protection de la vie privée : Comité exécutif des Services communs d'imagerie diagnostique Sécurité : Comité stratégique de cyberSanté Ontario

Tableau 1 : Organismes administratifs applicables

Terme ou sigle	Définition
DRS	Dépositaire de renseignements sur la santé.
RPS	Renseignements personnels sur la santé, tel que le terme est défini dans la *Loi de 2004 sur la protection des renseignements personnels sur la santé*.
LPRPS	*Loi de 2004 sur la protection des renseignements*

personnels sur la santé

7 Références et documents connexes

Loi de 2004 sur la protection des renseignements personnels sur la santé (LPRPS)
Politique pour la journalisation et la vérification du dossier de santé électronique et procédures connexes

eHealth Ontario

Politique sur les demandes de renseignements et les plaintes

Dossier de santé électronique

Version : 1.1

Nº de document : 3875

Ontario
eHealth Ontario

Gestion du document

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

Historique des approbations

APPROBATEURS	DATE D'APPROBATION
Membres du comité de protection de la vie privée ConnectingPrivacy	2014-06-26

Historique des révisions

NUMÉRO DE VERSION	DATE AAAA-MM-JJ	RÉSUMÉ DES CHANGEMENTS	AUTEUR DES CHANGEMENTS
0.01	2014-11-04	Première version établie en fonction de la politique harmonisée sur les demandes de renseignements et les plaintes du comité de protection de la vie privée ConnectingPrivacy, v1.1	Promila Gonsalves, analyste en protection de la vie privée, cyberSanté Ontario
1.0	2014-11-17	Version définitive	Urooj Kirmani, analyste principal en protection de la vie privée, cyberSanté Ontario

Table des matières

1 Objectif

Définir les politiques, les procédures et les pratiques s'appliquant à la réception et au suivi des demandes de renseignements et des plaintes ainsi qu'à la manière d'y répondre et à l'obtention des documents nécessaires pour tout ce qui concerne le dossier de santé électronique (DSE).

2 Portée

La présente politique et les procédures connexes s'appliquent aux demandes de renseignements et aux plaintes relatives au DSE. Le DSE est composé de la solution ConnexionOntario et du Dépôt d'imagerie diagnostique des services hospitaliers. La solution ConnexionOntario et le Dépôt d'imagerie diagnostique des services hospitaliers sont des dépôts ou des systèmes auxiliaires cliniques destinés à stocker et à rendre accessibles des renseignements personnels sur la santé (RPS) contenus dans les systèmes électroniques de renseignements sur la santé des dépositaires de ces renseignements[1].

La politique et les procédures connexes ne s'appliquent pas aux demandes de renseignements ni aux plaintes concernant tout système autre que le DSE ou tout renseignement autre que les RPS dans le DSE.

3 Politique

3.1 Fondements

3.1.1 La *Loi de 2004 sur la protection des renseignements personnels sur la santé* (LPRPS) exige qu'un dépositaire de renseignements sur la santé (DRS) qui n'est pas une personne physique, par exemple une société ou un partenariat, désigne une personne-ressource qui répondra aux demandes de renseignements sur les pratiques du DRS relatives aux renseignements, recevra les plaintes au sujet d'une contravention à la LPRPS et veillera à ce que tous les mandataires du DRS soient adéquatement informés des obligations que leur impose la LPRPS.

3.1.2 La LPRPS permet à un DRS qui est une personne physique de désigner une personne-ressource qui répondra aux demandes de renseignements sur les pratiques du DRS relatives aux renseignements, recevra les plaintes au sujet d'une contravention à la LPRPS et veillera à ce que tous les mandataires du DRS soient adéquatement informés des obligations que leur impose la LPRPS. Lorsqu'un DRS qui n'est pas une personne physique ne désigne pas de personne-ressource pour réaliser ces tâches, il doit les accomplir par lui-même.

3.1.3 Toute personne ayant des motifs raisonnables de croire qu'un DRS, cyberSanté Ontario ou un de leurs mandataires ou fournisseurs de services électroniques a contrevenu ou est sur le point de contrevenir à la LPRPS peut aussi formuler une plainte au commissaire à l'information et à la protection de la vie privée de l'Ontario.

3.1.4 La présente politique est les procédures connexes guideront toute personne dans l'exercice de son droit de faire une demande de renseignements ou de formuler une plainte concernant le DSE et permettront aux DRS et à cyberSanté Ontario de respecter les obligations que leur impose la LPRPS.

[1] Les divergences entre les exigences des politiques et des procédures de la solution ConnexionOntario et du Dépôt d'imagerie diagnostique des services hospitaliers sont indiquées dans la présente politique.

3.1.5 Les DRS et cyberSanté Ontario doivent avoir en place les politiques, les procédures et les pratiques sur la protection de la vie privée et la sécurité nécessaires pour les rendre conformes à leurs obligations aux termes de la LPRPS, des ententes applicables ainsi que de la présente politique et des procédures connexes.

3.1.6 Les DRS et cyberSanté Ontario doivent avoir en place des politiques, des procédures et des pratiques sur la protection de la vie privée et la sécurité qui respectent la LPRPS et informer leurs mandataires et leurs fournisseurs de services électroniques sur les politiques, les procédures et les pratiques imposées par la LPRPS.

3.1.7 cyberSanté Ontario doit avoir un programme leur permettant, à lui et aux DRS, de remplir leurs obligations par rapport à la réception et au suivi des demandes de renseignements et des plaintes ainsi qu'à la manière d'y répondre et à l'obtention des documents nécessaires pour ce qui concerne le DSE conformément à la LPRPS, aux ententes applicables ainsi qu'à la présente politique et aux procédures connexes.

3.1.8 Les DRS et cyberSanté Ontario doivent prendre les mesures nécessaires et raisonnables selon les circonstances afin que leurs mandataires et leurs fournisseurs de services électroniques se conforment à la LPRPS, aux ententes applicables ainsi qu'à la présente politique et aux procédures connexes.

4 Procédures

4.1 Procédures liées aux demandes de renseignements

Cas de demandes de renseignements selon la partie qui reçoit la demande

4.1.1 Lorsqu'un DRS reçoit directement une demande de renseignements ne concernant que lui-même ou ses mandataires ou ses fournisseurs de services électroniques[2], le DRS recevra la demande, rassemblera les documents nécessaires, effectuera le suivi et répondra directement au demandeur le plus tôt possible, mais, en toute circonstance, au plus tard trente (30) jours après réception de la demande de renseignements conformément aux politiques, aux procédures et aux pratiques internes.

4.1.2 Lorsque cyberSanté Ontario reçoit directement une demande de renseignements ne concernant qu'elle-même ou ses mandataires ou ses fournisseurs de services électroniques, cyberSanté Ontario recevra la demande, rassemblera les documents nécessaires, effectuera le suivi et répondra directement au demandeur le plus tôt possible, mais, en toute circonstance, au plus tard trente (30) jours après réception de la demande de renseignements conformément aux politiques, aux procédures et aux pratiques internes.

Réception d'une demande de renseignements par le DRS concernant cyberSanté Ontario, un autre DRS ou plus d'un DRS

4.1.3 Lorsqu'un DRS reçoit directement une demande de renseignements à laquelle il peut répondre concernant un autre DRS, plus d'un DRS, cyberSanté Ontario ou les mandataires ou les fournisseurs de services électroniques d'un autre DRS, de plus d'un DRS ou de cyberSanté Ontario, le DRS en question recevra la demande, rassemblera les documents nécessaires, effectuera le suivi et répondra directement au demandeur le plus tôt possible, mais, en toute circonstance, au plus tard trente (30) jours après réception de la demande de renseignements conformément aux politiques, aux procédures et aux pratiques internes.

4.1.4 Lorsqu'un DRS reçoit directement une demande de renseignements aux termes du paragraphe 4.1.3, mais qu'il n'est pas en mesure d'y répondre, le DRS doit, le plus tôt possible, mais, en toute circonstance, au plus tard quatre (4) jours après la réception de la demande, faire ce qui suit :

- informer le demandeur du fait que le DRS ne peut pas répondre à la demande de renseignements;
- fournir au demandeur l'information lui permettant de communiquer avec cyberSanté Ontario pour lui faire la demande de renseignements.

[2] Toutes les mentions dans la présente politique et les procédures connexes concernant les mandataires ou les fournisseurs de services électroniques d'un DRS font référence aux mandataires ou aux fournisseurs de services électroniques autres que cyberSanté Ontario ou les mandataires ou les fournisseurs de services électroniques de cyberSanté Ontario.

Réception d'une demande de renseignements par cyberSanté Ontario concernant un DRS ou plus d'un DRS

4.1.5 Lorsque cyberSanté Ontario reçoit directement une demande de renseignements à laquelle il peut répondre concernant un DRS ou plus d'un DRS ou les mandataires ou les fournisseurs de services électroniques d'un DRS ou de plus d'un DRS, cyberSanté Ontario recevra la demande, rassemblera les documents nécessaires, effectuera le suivi et répondra directement au demandeur le plus tôt possible, mais, en toute circonstance, au plus tard trente (30) jours après la réception de la demande de renseignements conformément aux politiques, aux procédures et aux pratiques internes.

4.1.6 Lorsque cyberSanté Ontario reçoit directement une demande de renseignements aux termes du paragraphe 4.1.5, mais qu'il n'est pas en mesure d'y répondre, cyberSanté Ontario doit faire ce qui suit :

- journaliser la réception de la demande de renseignements;
- informer le demandeur le plus tôt possible, mais, en toute circonstance, au plus tard quatre (4) jours après la réception de la demande de renseignements, des faits suivants :
    - cyberSanté Ontario a reçu la demande de renseignements;
    - cyberSanté Ontario transmettra la demande de renseignements au DRS ou aux DRS que concerne la demande de renseignements selon le cas;
    - le demandeur recevra une réponse à sa demande de renseignements de la part du DRS aux termes du paragraphe 4.1.7 ou de la part de cyberSanté Ontario, selon le cas, le plus tôt possible, mais, en toute circonstance, au plus tard trente (30) jours après la réception de la demande de renseignements par cyberSanté Ontario;
    - le demandeur recevra la date révisée à laquelle on répondra à sa demande de renseignements s'il est impossible de répondre dans les trente (30) jours suivant la réception de la demande de renseignements par cyberSanté Ontario;
- obtenir assez de renseignements du demandeur pour être en mesure de préparer la réponse à la demande de renseignements;
- obtenir auprès de demandeur la méthode de contact qu'il préfère et ses coordonnées pour qu'on lui fasse parvenir la réponse à sa demande de renseignements.

4.1.7 Sur réception d'une demande de renseignements ne concernant qu'un DRS, cyberSanté Ontario doit, le plus tôt possible, mais, en toute circonstance, au plus tard quatre (4) jours après la réception de la demande de renseignements, faire ce qui suit :

- transmettre la demande de renseignements au DRS que concerne la demande;
- informer le DRS du fait que la demande de renseignements ne le concerne que lui;
- fournir au DRS la date à laquelle la demande de renseignements a été reçue par cyberSanté Ontario;
- fournir au DRS l'information sur l'identité du demandeur, la méthode de contact qu'il préfère, les coordonnées à utiliser pour répondre à la demande de renseignements et toute l'information nécessaire pour préparer une réponse à la demande;
- informer le DRS du fait qu'il doit, le plus tôt possible, mais, en toute circonstance, au plus tard trente (30) jours après la réception de la demande de renseignements par cyberSanté Ontario, soit répondre directement au demandeur conformément à ses propres politiques, procédures et pratiques internes, soit fournir au demandeur une date révisée à laquelle on répondra à sa demande s'il est impossible de répondre à cette dernière dans le délai prescrit.

4.1.8 Sur réception d'une demande de renseignements transmise par cyberSanté Ontario ne concernant que le DRS, ce dernier doit faire ce qui suit :

- recevoir la demande, rassembler les documents nécessaires, effectuer le suivi et répondre directement au demandeur le plus tôt possible, mais, en toute circonstance, au plus tard trente (30) jours après la réception de la demande de renseignements par cyberSanté Ontario, conformément aux politiques, aux procédures et aux pratiques internes;
- fournir au demandeur une date révisée à laquelle on répondra à sa demande le plus tôt possible, mais, en toute circonstance, au plus tard trente (30) jours après la réception de la demande de renseignements par cyberSanté Ontario, s'il est impossible de répondre à la demande dans les trente (30) jours suivant la réception de la demande par cyberSanté Ontario;

- conserver une preuve montrant qu'on a répondu à la demande de renseignements en enregistrant une copie de la réponse ou un journal mentionnant qu'une réponse à été fournie.

4.1.9 Sur réception d'une demande de renseignements concernant plus d'un DRS, cyberSanté Ontario doit, le plus tôt possible, mais, en toute circonstance, au plus tard quatre (4) jours après la réception de la demande de renseignements, faire ce qui suit :

- transmettre la demande de renseignements à chaque DRS que concerne la demande;
- informer chaque DRS du fait que la demande de renseignements concerne plus d'un DRS;
- fournir à chaque DRS la date à laquelle la demande de renseignements a été reçue par cyberSanté Ontario;
- fournir à chaque DRS l'information sur l'identité du demandeur;
- informer chaque DRS du fait qu'il doit, le plus tôt possible, mais, en toute circonstance, au plus tard quatorze (14) jours après la réception de la demande de renseignements par cyberSanté Ontario, fournir à cyberSanté Ontario l'information nécessaire pour permettre à ce dernier de rédiger une suggestion de réponse à la demande de renseignements au nom de chaque DRS.

4.1.10 Sur réception d'une demande de renseignements transmise par cyberSanté Ontario concernant plus d'un DRS, chaque DRS que concerne la demande doit, le plus tôt possible, mais, en toute circonstance, au plus tard quatorze (14) jours après la réception de la demande de renseignements par cyberSanté Ontario, fournir à cyberSanté Ontario l'information nécessaire pour permettre à ce dernier de rédiger une suggestion de réponse à la demande de renseignements au nom de chaque DRS.

4.1.11 cyberSanté Ontario doit, le plus tôt possible, mais, en toute circonstance, au plus tard quatre (4) jours après la réception de l'information aux termes du paragraphe 4.1.10, rédiger une suggestion de réponse au demandeur et fournir la suggestion de réponse à chaque DRS que concerne la demande de renseignements afin d'en obtenir les commentaires.

4.1.12 Sur réception de la suggestion de réponse aux termes du paragraphe 4.1.11, chaque DRS doit fournir des commentaires à cyberSanté Ontario le plus tôt possible, mais, en toute circonstance, au plus tard quatre (4) jours après la réception de la suggestion de réponse. Si aucun commentaire n'est reçu dans les quatre (4) jours suivant la réception de la suggestion de réponse, cyberSanté Ontario supposera qu'il n'y a pas de commentaires.

4.1.13 Sur réception des commentaires sur la suggestion de réponse à la demande de renseignements concernant plus d'un DRS, cyberSanté Ontario doit, le plus tôt possible, mais, en toute circonstance, au plus tard quatre (4) jours après la réception des commentaires aux termes du paragraphe 4.1.10, répondre au demandeur.

4.1.14 Lorsqu'un DRS ou plus d'un DRS ne fournit pas l'information nécessaire pour que cyberSanté Ontario réponde à la demande de renseignements conformément au délai prescrit au paragraphe 4.1.10, cyberSanté Ontario doit fournir un avis écrit au demandeur pour lui signaler qu'un DRS ou plus d'un DRS n'a pas répondu à la demande de renseignements et que la personne peut faire une demande de renseignements ou une plainte à un DRS ou à plus d'un DRS n'ayant pas répondu ou déposer une plainte auprès du commissaire à l'information et à la protection de la vie privée de l'Ontario.

4.1.15 Lorsqu'une demande de renseignements concerne plus d'un DRS, cyberSanté Ontario doit fournir au demandeur une date révisée à laquelle on répondra à sa demande de renseignements s'il est impossible de répondre dans les trente (30) jours suivant la réception de la demande de renseignements par cyberSanté Ontario.

4.2 Procédures liées aux plaintes

Cas de plaintes selon la partie qui reçoit la plainte

4.2.1 Lorsqu'un DRS reçoit directement une plainte ne concernant que lui-même ou ses mandataires ou ses fournisseurs de services électroniques, le DRS recevra la plainte, rassemblera les documents nécessaires, effectuera le suivi, fera enquête, trouvera une solution au problème et répondra directement au plaignant le plus tôt possible, mais, en toute circonstance, au plus tard trente (30) jours après la réception de la plainte conformément aux politiques, aux procédures et aux pratiques internes.

4.2.2 Lorsque cyberSanté Ontario reçoit directement une plainte ne concernant que lui-même ou ses mandataires ou ses fournisseurs de services électroniques, cyberSanté Ontario recevra la plainte, rassemblera les documents nécessaires, effectuera le suivi, fera enquête, trouvera une solution au problème et répondra directement au plaignant le plus tôt possible, mais, en toute circonstance, au plus tard trente (30) jours après réception de la plainte conformément aux politiques, aux procédures et aux pratiques internes.

Réception d'une plainte par le DRS concernant cyberSanté Ontario, un autre DRS ou plus d'un DRS

4.2.3 Lorsqu'un DRS reçoit directement une plainte concernant un autre DRS, plus d'un DRS, cyberSanté Ontario ou les mandataires ou les fournisseurs de services électroniques d'un autre DRS, de plus d'un DRS ou de cyberSanté Ontario, le DRS en question doit, le plus tôt possible, mais, en toute circonstance, au plus tard quatre (4) jours après la réception de la plainte, faire ce qui suit :

- informer le plaignant du fait que le DRS ne peut pas répondre à la plainte;
- fournir au plaignant l'information lui permettant de communiquer avec cyberSanté Ontario pour déposer sa plainte.

Réception d'une plainte par cyberSanté Ontario concernant un DRS ou plus d'un DRS

4.2.4 Lorsque cyberSanté Ontario reçoit directement une plainte concernant un DRS ou plus d'un DRS ou les mandataires ou les fournisseurs de services électroniques d'un DRS ou de plus d'un DRS, il doit faire ce qui suit :

- journaliser la réception de la plainte;
- informer le plaignant le plus tôt possible, mais, en toute circonstance, au plus tard quatre (4) jours après la réception de la plainte, des faits suivants :
  - cyberSanté Ontario a reçu la plainte;
  - cyberSanté Ontario transmettra la plainte au DRS ou aux DRS que concerne la plainte selon le cas;
  - le plaignant recevra une réponse à sa plainte de la part du DRS aux termes du paragraphe 4.2.7 ou de la part de cyberSanté Ontario, selon le cas, le plus tôt possible, mais, en toute circonstance, au plus tard trente (30) jours après la réception de la plainte par cyberSanté Ontario;
  - le plaignant recevra la date révisée à laquelle on répondra à sa plainte s'il est impossible de répondre dans les trente (30) jours suivant la réception de la plainte par cyberSanté Ontario;
- obtenir assez de renseignements du plaignant pour être en mesure de préparer la réponse à la plainte;
- obtenir auprès de plaignant la méthode de contact qu'il préfère et ses coordonnées pour qu'on lui fasse parvenir la réponse à sa plainte.

4.2.5 Lorsque cyberSanté Ontario reçoit une plainte anonyme, cette plainte doit être signalée, gérée et résolue après enquête conformément à la *Politique de gestion des atteintes à la confidentialité du dossier de santé électronique* ou à la *Politique de gestion des atteintes à la sécurité des renseignements du dossier de santé électronique* et leurs procédures connexes, ce qui comprend les modifications qui y sont apportées de temps à autre. cyberSanté Ontario doit prendre toutes les mesures raisonnables pour informer le plaignant anonyme des limites possibles de toute enquête à la suite d'une plainte anonyme, ce qui comprend :

- les limites relatives à l'enquête à effectuer à la suite d'une plainte liée au dossier de santé électronique d'une personne anonyme;
- les limites quant à la possibilité de répondre de manière proactive directement au plaignant anonyme.

4.2.6 Sur réception d'une plainte ne concernant qu'un DRS, cyberSanté Ontario doit, le plus tôt possible, mais, en toute circonstance, au plus tard quatre (4) jours après la réception de la plainte, faire ce qui suit :

- transmettre la plainte au DRS que concerne la plainte;
- informer le DRS du fait que la plainte ne le concerne que lui;
- fournir au DRS la date à laquelle la plainte a été reçue par cyberSanté Ontario;
- fournir au DRS l'information sur l'identité du plaignant, la méthode de contact qu'il préfère, les coordonnées à utiliser pour répondre à la plainte et tous les renseignements nécessaires pour préparer une réponse à la plainte;
- informer le DRS du fait qu'il doit, le plus tôt possible, mais, en toute circonstance, au plus tard trente (30) jours après la réception de la plainte par cyberSanté Ontario, soit répondre directement au plaignant conformément à ses propres politiques, procédures et pratiques internes, soit fournir au plaignant une date révisée à laquelle on répondra à sa plainte s'il est impossible de répondre à cette dernière dans le délai prescrit.

4.2.7 Sur réception d'une plainte transmise par cyberSanté Ontario ne concernant que le DRS, ce dernier doit faire ce qui suit :

- recevoir la plainte, rassembler les documents nécessaires, effectuer le suivi, faire enquête, trouver une solution au problème et répondre directement au plaignant le plus tôt possible, mais, en toute circonstance, au plus tard trente (30) jours après la réception de la plainte par cyberSanté Ontario, conformément aux politiques, aux procédures et aux pratiques internes du DRS;
- fournir au plaignant une date révisée à laquelle on répondra à sa plainte le plus tôt possible, mais, en toute circonstance, au plus tard trente (30) jours après la réception de la plainte par cyberSanté Ontario s'il est impossible de répondre à la plainte dans les trente (30) jours suivant la réception de la plainte par cyberSanté Ontario;
- conserver une preuve montrant qu'on a répondu à la plainte en enregistrant une copie de la réponse ou un journal mentionnant qu'une réponse à été fournie.

4.2.8 Sur réception d'une plainte concernant plus d'un DRS, cyberSanté Ontario doit, le plus tôt possible, mais, en toute circonstance, au plus tard quatre (4) jours après la réception de la plainte, faire ce qui suit :

- transmettre la plainte à chaque DRS que concerne la plainte;
- informer chaque DRS du fait que la plainte concerne plus d'un DRS;
- fournir à chaque DRS la date à laquelle la plainte a été reçue par cyberSanté Ontario;
- fournir à chaque DRS l'information sur l'identité du plaignant;
- informer chaque DRS du fait qu'il doit, le plus tôt possible, mais, en toute circonstance, au plus tard quatorze (14) jours après la réception de la plainte par cyberSanté Ontario, fournir à cyberSanté Ontario l'information nécessaire pour permettre à ce dernier de déterminer s'il faut faire enquête et, s'il est décidé qu'aucune enquête n'aura lieu, de rédiger une suggestion de réponse au plaignant au nom de chaque DRS.

4.2.9 Sur réception d'une plainte transmise par cyberSanté Ontario concernant plus d'un DRS, chaque DRS que concerne la plainte doit, le plus tôt possible, mais, en toute circonstance, au plus tard quatorze (14) jours après la réception de la plainte par cyberSanté Ontario, fournir à cyberSanté Ontario l'information nécessaire pour permettre à ce dernier de déterminer s'il faut faire enquête et, s'il est décidé qu'aucune enquête n'aura lieu, de rédiger une suggestion de réponse à la plainte au nom de chaque DRS.

4.2.10 cyberSanté Ontario doit, le plus tôt possible, mais, en toute circonstance, au plus tard quatre (4) jours après la réception de l'information aux termes du paragraphe 4.2.9, déterminer s'il faut faire enquête. Il doit y avoir enquête lorsque la plainte porte sur une atteinte à la vie privée confirmée ou soupçonnée ou une atteinte à la sécurité confirmée ou soupçonnée qui s'est produite ou est sur le point de se produire concernant le DSE.

4.2.11 Lorsque la plainte porte sur plus d'un DRS et que cyberSanté Ontario a déterminé qu'il fallait faire enquête aux termes du paragraphe 4.2.10, cyberSanté Ontario doit informer chaque DRS que concerne la plainte des faits suivants :

- cyberSanté Ontario a déterminé qu'il fallait faire enquête;
- la plainte porte sur une atteinte à la vie privée confirmée ou soupçonnée ou une atteinte à la sécurité confirmée ou soupçonnée qui s'est produite ou est sur le point de se produire concernant le DSE;
- on signalera, gérera et résoudra la plainte après enquête et on divulguera l'information conformément à la *Politique de gestion des atteintes à la confidentialité du dossier de santé électronique* et aux procédures connexes ou on signalera, gérera et résoudra la plainte après enquête conformément à la *Politique de gestion des atteintes à la sécurité des renseignements du dossier de santé électronique* et aux procédures connexes, ce qui comprend les modifications qui y sont apportées de temps à autre.

4.2.12 Lorsque la plainte concerne une atteinte à la vie privée confirmée ou soupçonnée, cette atteinte doit être signalée, gérée et résolue après enquête, et l'information doit être divulguée conformément à la *Politique de gestion des atteintes à la confidentialité du dossier de santé électronique* et aux procédures connexes, ce qui comprend les modifications qui y sont apportées de temps à autre.

4.2.13 Lorsque la plainte concerne une atteinte à la sécurité confirmée ou soupçonnée, cette atteinte doit être signalée, gérée et résolue après enquête conformément à la *Politique de gestion des atteintes à la sécurité des renseignements du dossier de santé électronique* et aux procédures connexes, ce qui comprend les modifications qui y sont apportées de temps à autre.

4.2.14 Lorsqu'une plainte concerne une atteinte à la sécurité confirmée ou soupçonnée ou qu'elle concerne une atteinte à la vie privée confirmée ou soupçonnée et que la plainte est formulée par une personne autre que celle à qui appartiennent les RPS, cyberSanté Ontario doit répondre au plaignant le plus tôt possible, mais, en toute circonstance, au plus tard cinq (5) jours après la réception du rapport écrit approuvé par l'organisme de surveillance applicable conformément à la *Politique de gestion des atteintes à la confidentialité du dossier de santé électronique* ou à la *Politique de gestion des atteintes à la sécurité des renseignements du dossier de santé électronique* et aux procédures connexes, ce qui comprend les modifications qui y sont apportées de temps à autre. La réponse doit au minimum inclure les éléments suivants :

- un accusé de réception de la plainte;
- une mention selon laquelle une enquête a été effectuée en réponse à la plainte;
- une mention selon laquelle il y a eu ou non une atteinte à la vie privée ou une atteinte à la sécurité et, le cas échéant, une description de l'atteinte, de sa gravité et des circonstances dans lesquelles elle est survenue;
- un sommaire des résultats de l'enquête et des mesures qui ont été ou seront mises en œuvre pour résoudre le cas d'atteinte à la vie privée ou d'atteinte à la sécurité et prévenir tout incident similaire à l'avenir;
- le nom et les coordonnées de la personne ou des personnes à qui le plaignant peut poser des questions ou faire part de ses préoccupations;
- une mention informant le plaignant de la possibilité de déposer une plainte au commissaire à l'information et à la protection de la vie privée de l'Ontario.

4.2.15 Lorsque cyberSanté Ontario a déterminé qu'il n'était pas nécessaire de faire enquête aux termes du paragraphe 4.2.10, il doit, le plus tôt possible, mais, en toute circonstance, au plus tard quatre (4) jours après la réception de l'information aux termes du paragraphe 4.2.9, faire ce qui suit :

- informer chaque DRS que concerne la plainte du fait que cyberSanté Ontario a déterminé qu'il n'était pas nécessaire de faire enquête;
- fournir à chaque DRS la suggestion de réponse au plaignant et informer chaque DRS du fait qu'il doit, le plus tôt possible, mais, en toute circonstance, au plus tard quatre (4) jours après la réception de la suggestion de réponse, fournir des commentaires sur la suggestion de réponse à cyberSanté Ontario pour que cette dernière réponde au plaignant au nom de chaque DRS.

4.2.16 Sur réception de la suggestion de réponse aux termes du paragraphe 4.2.15, chaque DRS doit fournir des commentaires à cyberSanté Ontario le plus tôt possible, mais, en toute circonstance, au plus tard quatre (4) jours après la réception de la suggestion de réponse. Si aucun commentaire n'est reçu dans les quatre (4) jours suivant la réception de la suggestion de réponse, cyberSanté Ontario supposera qu'il n'y a pas de commentaires.

4.2.17 Sur réception des commentaires sur la suggestion de réponse à la plainte concernant plus d'un DRS, cyberSanté Ontario doit, le plus tôt possible, mais, en toute circonstance, au plus tard quatre (4) jours après la réception des commentaires, répondre au plaignant. La réponse doit au minimum inclure les éléments suivants :

- une réponse à la plainte;
- le nom et les coordonnées de la personne ou des personnes à qui le plaignant peut poser des questions ou faire part de ses préoccupations;
- une mention informant le plaignant de la possibilité de déposer une plainte au commissaire à l'information et à la protection de la vie privée de l'Ontario.

4.2.18 Lorsqu'un DRS ou plus d'un DRS ne fournit pas l'information nécessaire pour que cyberSanté Ontario réponde à la plainte conformément au délai prescrit au paragraphe 4.2.9, cyberSanté Ontario doit fournir un avis écrit au plaignant pour lui signaler qu'un DRS ou plus d'un DRS n'a pas répondu à la plainte et que la personne peut faire une plainte à un DRS ou à plus d'un DRS n'ayant pas répondu ou déposer une plainte auprès du commissaire à l'information et à la protection de la vie privée de l'Ontario.

4.2.19 cyberSanté Ontario doit fournir au plaignant une date révisée à laquelle on répondra à sa plainte s'il est impossible de répondre dans les trente (30) jours après la réception de la plainte par cyberSanté Ontario.

5 Application[3]

5.1.1 Tous les cas de non-respect seront examinés par le comité de protection de la vie privée et de sécurité applicable. Le comité de protection de la vie privée et de sécurité applicable recommandera la voie à suivre à l'organisme de surveillance applicable.

5.1.2 L'organisme de surveillance applicable a le pouvoir d'imposer les sanctions appropriées, ce qui peut inclure la cessation des ententes applicables avec le DRS ou la cessation des privilèges d'accès des mandataires et des fournisseurs de services électroniques et une demande de mesures correctives.

6 Glossaire

Dossier de santé électronique (DSE)
Ensemble de la solution ConnexionOntario et du Dépôt d'imagerie diagnostique des services hospitaliers, soit des dépôts ou des systèmes auxiliaires cliniques destinés à stocker et à rendre accessibles des renseignements personnels sur la santé contenus dans les systèmes électroniques de renseignements sur la santé des dépositaires de ces renseignements de manière à ne créer qu'un seul dépôt.

Plainte
Question soulevée par toute personne concernant le dossier de santé électronique, ce qui comprend, sans s'y limiter, la conformité à la *Loi sur la protection des renseignements personnels sur la santé*, les ententes applicables ainsi que les politiques, les procédures et les pratiques liées au dossier de santé électronique.

Fournisseur de services électroniques
Personne qui fournit des biens ou des services dans le but de permettre à un dépositaire de renseignements sur la santé d'employer des moyens électroniques de recueillir, d'utiliser, de modifier, de divulguer, de conserver ou d'éliminer des renseignements personnels sur la santé et qui comprend un fournisseur de réseau d'information sur la santé.

Demande de renseignements
Question posée par toute personne concernant le dossier de santé électronique, ce qui comprend, sans s'y limiter, les thèmes suivants :

- quand, comment et pourquoi les renseignements personnels sur la santé d'un dossier de santé électronique sont recueillis, utilisés, divulgués, consultés, manipulés ou employés d'une quelconque autre manière;
- les mesures de protection administratives, techniques et matérielles pour les renseignements personnels sur la santé contenus dans le dossier de santé électronique ainsi que les pratiques adoptées à leur égard;
- les politiques, les procédures et les pratiques liées au dossier de santé électronique;
- la conformité à la *Loi sur la protection des renseignements personnels sur la santé*, les ententes applicables ainsi que les politiques, les procédures et les pratiques liées au dossier de santé électronique.

Atteinte à la vie privée
Le terme *atteinte à la vie privée* a le même sens que dans la *Politique de gestion des atteintes à la confidentialité du dossier de santé électronique* ainsi que les procédures connexes, ce qui comprend les modifications qui y sont apportées de temps à autre.

Atteinte à la sécurité
Le terme *atteinte à la sécurité* a le même sens que dans la *Politique de gestion des atteintes à la sécurité des renseignements du dossier de santé électronique* ainsi que ses procédures connexes, ce qui comprend les modifications qui y sont apportées de temps à autre.

[3] Les références au comité de protection de la vie privée et de sécurité applicable et à l'organisme de surveillance applicable se trouvent au *Tableau 1 : Organismes administratifs applicables*.

Structure d'administration de la politique	Solution ConnexionOntario	Dépôt des Services communs d'imagerie diagnostique
Comité de protection de la vie privée et de sécurité applicable	Protection de la vie privée : Comité de protection de la vie privée (Connecting Privacy) Sécurité : Comité de sécurité (Connecting Security)	Protection de la vie privée : Groupe de travail sur la protection de la vie privée et la sécurité des Services communs d'imagerie diagnostique Sécurité : Comité de sécurité (Connecting Security)
Organisme de surveillance applicable	Protection de la vie privée : Comité directeur de ConnexionOntario Sécurité : Comité stratégique de cyberSanté Ontario	Protection de la vie privée : Comité exécutif des Services communs d'imagerie diagnostique Sécurité : Comité stratégique de cyberSanté Ontario

Tableau 1 : Organismes administratifs applicables

Terme ou sigle	Définition
DRS	Dépositaire de renseignements sur la santé
RPS	Renseignements personnels sur la santé, tel que le terme est défini dans la *Loi de 2004 sur la protection des renseignements personnels sur la santé*
LPRPS	*Loi de 2004 sur la protection des renseignements personnels sur la santé*

7 Références et documents connexes

Loi de 2004 sur la protection des renseignements personnels sur la santé (LPRPS)
Politique de gestion des atteintes à la confidentialité du dossier de santé électronique et procédures connexes
Politique de gestion des atteintes à la sécurité des renseignements du dossier de santé électronique et procédures connexes

eHealth Ontario

Politique sur la journalisation et la surveillance

Dossier de santé électronique

Version : 1.1

Nº de document : 3876

Ontario
eHealth Ontario

Gestion du document

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

Historique des approbations

APPROBATEURS	DATE D'APPROBATION
Membres du Comité ConnectingPrivacy	24 juin 2014

Historique des révisions

NUMÉRO DE VERSION	DATE AAAA-MM-JJ	Résumé des changements	AUTEUR DES CHANGEMENTS
1.0	2014-11-17	Version définitive	Urooj Kirmani, analyste principal en protection de la vie privée, cyberSanté Ontario
0.01	2014-11-04	Première version établie en fonction de la Politique harmonisée pour la journalisation et la surveillance v. 1.1 du Comité ConnectingPrivacy.	Promila Gonsalves, analyste en protection de la vie privée, cyberSanté Ontario

1 Table des matières

1 Objectif

Définir les politiques, les procédures et les pratiques qui s'appliquent à la journalisation, à la surveillance et au contrôle de tous les cas dans lesquels :

- l'intégralité ou une partie des renseignements personnels sur la santé (RPS) du dossier de santé électronique (DSE) a été consultée, manipulée ou autrement traitée[1];
- l'intégralité ou une partie des RPS du DSE est transférée à un dépositaire de renseignements sur la santé (DRS);
- l'intégralité ou une partie des RPS du DSE est divulguée à un DRS et collectée par ce dernier après dérogation à la directive sur le consentement; et
- une directive sur le consentement est dressée, modifiée ou retirée du DSE.

Faciliter la détection et l'enquête des atteintes à la confidentialité ou à la sécurité, réelles ou suspectées.

2 Portée

La présente politique et ses procédures connexes s'appliquent à la journalisation, à la surveillance et au contrôle du dossier de santé électronique dans le but de faciliter la détection et l'enquête sur les atteintes à la confidentialité ou à la sécurité, réelles ou suspectées, des RPS du DSE. Le DSE est composé de la solution ConnexionOntario et du Dépôt du Service commun d'imagerie diagnostique. La solution ConnexionOntario et le Dépôt du service commun d'imagerie diagnostique sont le dépôt clinique ou des systèmes auxiliaires cliniques destinés à stocker et à rendre accessibles des renseignements personnels sur la santé (RPS) contenus dans les systèmes électroniques de renseignements sur la santé des dépositaires de ces renseignements[2].

La présente politique et ses procédures connexes ne s'appliquent à la journalisation, à la surveillance et au contrôle d'aucun système autre que le DSE.

3 Politique

3.1 Fondements

3.1.1 La *Loi de 2004 sur la protection des renseignements personnels sur la santé, 2004* (LPRPS) exige des DRS qu'ils conservent, transfèrent et éliminent les RPS d'une façon sûre et qu'ils prennent des mesures raisonnables dans les circonstances pour s'assurer que les RPS sous leur garde ou leur contrôle sont protégés contre le vol, la perte et l'utilisation ou la divulgation non autorisées.

3.1.2 La LPRPS exige que cyberSanté Ontario mette en œuvre des sauvegardes pour protéger la sécurité et la confidentialité des RPS des DSE, y compris pour protéger les RPS contre toute utilisation ou divulgation non autorisées.

3.1.3 Les DRS et cyberSanté Ontario doivent avoir en place et maintenir les politiques, les procédures et les pratiques nécessaires en matière de confidentialité et de sécurité pour leur permettre de se conformer à leurs obligations en vertu de la LPRPS, des accords applicables en la matière et de la présente politique et de ses procédures connexes.

---

[1] Pour plus de précision, consulter, manipuler ou autrement traiter comprend la collecte, l'utilisation ou la divulgation, le cas échéant.

[2] Les divergences d'exigences de la politique et de la procédure entre la solution ConnexionOntario et le Dépôt du service commun d'imagerie diagnostique sont soulignées dans la politique.

3.1.4 Les DRS et cyberSanté Ontario doivent avoir en place et maintenir des politiques, des procédures et des pratiques en matière de confidentialité et de sécurité qui se conforment à la LPRPS et sensibiliser leurs mandataires et leurs fournisseurs de services électroniques à ces politiques, ces procédures et ces pratiques comme l'exige la LPRPS.

3.1.5 cyberSanté Ontario devra avoir en place un programme et fournir les outils pour permettre aux DRS de satisfaire aux exigences en matière de vérification et de surveillance conformément à la LPRPS, aux accords applicables en la matière et à la présente politique et à ses procédures connexes.

3.1.6 cyberSanté Ontario devra avoir en place un programme et des outils pour lui permettre de satisfaire à ses exigences en matière de journalisation, de vérification et de surveillance conformément à la LPRPS, aux accords applicables en la matière et à la présente politique et à ses procédures connexes.

3.1.7 Les DRS et cyberSanté Ontario prendront les mesures raisonnables dans les circonstances pour s'assurer que leurs mandataires et fournisseurs de services électroniques se conforment à la LPRPS, aux accords applicables en la matière et à la présente politique et à ses procédures connexes.

3.1.8 La présente politique et ses procédures connexes aideront les DRS et cyberSanté Ontario à satisfaire à leurs obligations légales grâce à la journalisation, à la vérification et au contrôle des DSE.

4 Procédures

4.1 Procédure relative à la journalisation par cyberSanté Ontario

4.1.1 cyberSanté Ontario s'assurera d'inscrire aux dossiers de santé électronique tous les cas où :

- l'intégralité ou une partie des renseignements personnels sur la santé (RPS) du dossier de santé électronique (DSE) a été consultée, manipulée ou autrement traitée;
- l'intégralité ou une partie des RPS du DSE est transférée à un dépositaire de renseignements sur la santé (DRS);
- l'intégralité ou une partie des RPS du DSE est divulguée et collectée par un DRS après avoir dérogé à la directive sur le consentement; et
- une directive sur le consentement est faite, retirée du DSE ou modifiée.

4.1.2 cyberSanté Ontario s'assurera que le journal de tous les cas où l'intégralité ou une partie des RPS du DSE est consultée, manipulée ou autrement traitée précise :

- la personne que les RPS concernent;
- le type de RPS consultés, manipulés ou autrement traités;
- toutes les personnes qui ont consulté, manipulé ou autrement traité les RPS;
- toute personne au nom de laquelle les RPS ont été consultés, manipulés ou autrement traités, le cas échéant; et
- la date, l'heure et l'endroit où ont eu lieu cette consultation, cette manipulation ou ce traitement.

4.1.3 cyberSanté Ontario s'assurera que le journal de tous les cas où l'intégralité ou une partie des RPS du DSE est transférée à un DRS précise :

- la personne que les RPS concernent;
- Le type de RPS transférés;
- le DRS qui demande que les RPS soient transférés;
- la date et l'heure à laquelle les RPS ont été transférés; et
- l'endroit auquel les RPS ont été transférés.

4.1.4 cyberSanté Ontario s'assurera que le journal de tous les cas où l'intégralité ou une partie des RPS du DSE est divulguée ou collectée par un DRS après dérogation à la directive sur le consentement précise :

- le DRS qui a divulgué les RPS;
- le DRS qui a collecté les RPS;
- tout agent qui a collecté les RPS au nom d'un DRS;
- la personne que les RPS concernent;
- le type de RPS divulgués;
- la date et l'heure à laquelle les RPS ont été divulgués; et
- la raison de cette divulgation.

4.1.5 cyberSanté Ontario s'assurera que le journal de tous les cas où une directive sur le consentement a été faite, retirée ou modifiée dans le DSE précise :

- la personne ou le mandataire spécial (MS) de la personne qui a dressé, retiré ou modifié la directive sur le consentement;
- la directive sur le consentement mise en œuvre selon les instructions que la personne ou le MS de la personne a fournies;
- le DRS, le mandataire ou toute autre personne à qui la directive est donnée, retirée ou modifiée; et
- la date et l'heure à laquelle la directive sur le consentement a été donnée, retirée ou modifiée.

4.1.6 cyberSanté Ontario fournira au Commissaire à l'information et à la protection de la vie privée/Ontario, à sa demande et aux fins de la partie VI de la LPRPS, les journaux établis au paragraphe 4.1.1 qui contiennent le contenu établi aux paragraphes 4.1.2 à 4.1.5.

4.1.7 Avant de fournir les journaux décrits au paragraphe 4.1.6 au Commissaire à l'information et à la protection de la vie privée/Ontario, cyberSanté Ontario en avisera le ou les DRS mentionnés dans les journaux ou dont le mandataire ou le fournisseur de services électroniques est mentionné dans le journal.

4.1.8 cyberSanté Ontario fournira les journaux établis au paragraphe 4.1.1 qui contiennent le contenu établi aux paragraphes 4.1.2 à 4.1.5 à la demande d'un DRS qui en a besoin pour en vérifier et surveiller la conformité à la LPRPS, aux accords applicables en la matière et à la présente politique et ses procédures connexes.

4.1.9 cyberSanté Ontario s'assurera que les journaux sont conservés, transférés et éliminés d'une manière qui permet la conformité à la LPRPS, à la *Politique sur la conservation des dossiers électroniques de santé* (à rédiger) et à la *Politique sur la sécurité des renseignements du dossier de santé électronique* et ses procédures connexes, telles que modifiées de temps à autre.

4.2 Procédure relative à la vérification et à la surveillance par cyberSanté Ontario

4.2.1 cyberSanté Ontario effectuera la vérification et la surveillance décrites aux paragraphes 4.2.2 à 4.2.5 pour assurer la conformité à la LPRPS, aux accords applicables en la matière et aux politiques, aux procédures et aux pratiques mises en œuvre pour les DSE conformément aux critères de vérification et de surveillance établis par le comité de protection de la vie privée et de sécurité applicable.

4.2.2 cyberSanté Ontario vérifiera et surveillera les cas où l'intégralité ou une partie des RPS du DSE est consultée, manipulée ou autrement traitée par les mandataires ou les fournisseurs de services électroniques de cyberSanté Ontario.

4.2.3 cyberSanté Ontario vérifiera et surveillera les autres cas où l'intégralité ou une partie des RPS du DSE est consultée, manipulée ou autrement traitée.

4.2.4 cyberSanté Ontario vérifiera et surveillera les cas où l'intégralité ou une partie des RPS du DSE est transférée à un DRS.

4.2.5 cyberSanté Ontario vérifiera, surveillera et alertera le DRS qui les a collectés toutes les fois que l'intégralité ou une partie des RPS du DSE est divulguée et collectée par le DRS après dérogation à la directive sur le consentement conformément à la *Politique de gestion du consentement relatif au dossier de santé électronique* et ses procédures connexes, telles que modifiées de temps à autre.

4.2.6 cyberSanté Ontario soumettra au Commissaire à l'information et à la protection de la vie privée/Ontario, au moins chaque année, un rapport écrit sur tous les cas où l'intégralité ou une partie des RPS du DSE est divulguée ou collectée par un DRS en dérogation à la directive sur le consentement.

4.2.7 cyberSanté Ontario vérifiera et surveillera tous les cas où une directive sur le consentement a été faite, retirée ou modifiée dans le DSE.

4.2.8 cyberSanté Ontario, lorsqu'il détecte une atteinte à la confidentialité réelle ou suspectée, appliquera la *Politique sur la gestion des atteintes à la vie privée du dossier de santé électronique* et ses procédures connexes, telles que modifiées de temps en autre. cyberSanté Ontario, lorsqu'il détecte une atteinte à la sécurité réelle ou suspectée, appliquera la *Politique sur la gestion des incidents de sécurité relatifs aux renseignements du dossier de santé électronique* et ses procédures connexes, telles que modifiées de temps à autre.

4.3 Procédure relative aux outils de vérification et de surveillance par cyberSanté Ontario

4.3.1 cyberSanté Ontario mettra à la disposition des DRS des outils et rapports de vérification et de surveillance pour leur permettre de satisfaire à leurs obligations en matière de vérification et de surveillance en vertu de la LPRPS, des accords applicables en la matière et de la présente politique et de ses procédures connexes.

4.3.2 Les outils et rapports de vérification et de surveillance qui seront mis à disposition par cyberSanté Ontario seront d'un format sûr, inaltérable et largement répandu.

4.3.3 cyberSanté Ontario automatisera la vérification et la surveillance du DSE lorsqu'il existera une technologie à l'appui d'une vérification et d'une surveillance proactives du DSE.

4.4 Procédure relative à la vérification et à la surveillance par les DRS

4.4.1 Les DRS effectueront les activités de vérification et de surveillance décrites aux paragraphes 4.4.2 à 4.4.4 pour assurer la conformité à la LPRPS, aux accords applicables en la matière et aux politiques, aux procédures et aux pratiques mises en œuvre pour les DSE conformément aux critères de vérification et de surveillance établis par le comité de protection de la vie privée et de sécurité applicable.

4.4.2 Tous les DRS vérifieront et surveilleront les cas où l'intégralité ou une partie des RPS du DSE est consultée, manipulée ou autrement traitée par les mandataires ou les fournisseurs de services électroniques des DRS autres que les mandataires ou les fournisseurs de services électroniques de cyberSanté Ontario.

4.4.3 Tous les DRS vérifieront et surveilleront tous les cas où le DRS et les mandataires ou les fournisseurs de services électroniques du DRS, autres que les mandataires ou les fournisseurs de services électroniques de cyberSanté Ontario, ont mis en œuvre les instructions d'une personne ou de son mandataire spécial de dresser, de retirer ou de modifier une directive sur le consentement dans le DSE.

4.4.4 Les DRS qui ont créé des RPS au DSE et y ont contribué devront, en plus de la vérification et de la surveillance des paragraphes 4.4.2 et 4.4.3, vérifier et surveiller :

- tous les autres cas dans lesquels l'intégralité ou une partie des RPS du DSE que le DRS a créés et auxquels il a contribué a été consultée, manipulée ou autrement traitée; et
- tous les cas dans lesquels une directive sur le consentement a été dressée, retirée ou modifiée relative aux RPS créés ou ajoutés au DSE par un DRS.

4.4.5 Le DRS, lorsqu'il détecte une atteinte à la confidentialité réelle ou suspectée, suivra la *Politique sur la gestion des atteintes à la confidentialité du dossier de santé électronique* et ses procédures connexes, telles que modifiées de temps à autre. Le DRS, lorsqu'il détecte une atteinte à la sécurité réelle ou suspectée, suivra la *Politique sur la gestion des atteintes à la sécurité du dossier de santé électronique* et ses procédures connexes, telles que modifiées de temps à autre.

4.4.6 À la réception d'un avis de cyberSanté Ontario que le DRS a collecté l'intégralité ou une partie des RPS du DSE en dérogation à une directive sur le consentement, le DRS se conformera à ses obligations en vertu de la LPRPS et de la *Politique de gestion du consentement relatif au dossier de santé électronique* et ses procédures connexes, telles que modifiées de temps à autre.

4.5 Procédure pour établir les critères de vérification et de surveillance

4.5.1 Le comité de protection de la vie privée et de sécurité applicable devra établir les critères de vérification et de surveillance qu'utiliseront cyberSanté Ontario et les DRS, selon le cas, avant que tout RPS du DSE soit consulté, manipulé ou autrement traité. Le comité de protection de la vie privée et de sécurité applicable consultera l'organisme de surveillance pertinent sur les critères de vérification et de surveillance.

4.5.2 Les critères établis en vertu du paragraphe 4.5.1 permettront aux DRS et à cyberSanté Ontario de se conformer à leurs obligations en vertu de la LPRPS, des accords applicables en la matière et des politiques, des procédures et des pratiques mises en œuvre pour le DSE, et correspondront aux normes et aux pratiques exemplaires de l'industrie et seront fondés sur l'évaluation des menaces et des risques que posent les RPS du DSE.

5 Exécution[3]

5.1.1 Tous les cas de non-conformité seront examinés par le comité de protection de la vie privée et de sécurité applicable. Le comité de protection de la vie privée et de sécurité applicable recommandera les mesures appropriées à l'organisme de surveillance pertinent.

5.1.2 L'organisme de surveillance pertinent a le pouvoir d'imposer les sanctions appropriées, jusqu'à et y compris la fin de l'accord en la matière avec le DRS ou la fin des privilèges d'accès des mandataires et fournisseurs de services électroniques, et d'exiger la mise en œuvre de mesures correctrices.

6 Glossaire

Dossier de santé électronique (DSE)
Ensemble de la solution ConnexionOntario et du Dépôt du Service commun d'imagerie diagnostique, soit des dépôts ou des systèmes auxiliaires cliniques destinés à stocker et à rendre accessibles des renseignements personnels sur la santé contenus dans les systèmes électroniques de renseignements sur la santé des dépositaires de ces renseignements de manière à ne créer qu'un seul dépôt.

Directive sur le consentement
Directive sur le consentement a la même signification que dans la *Politique de gestion du consentement relatif au dossier de santé électronique* et ses procédures connexes, telles que modifiées de temps à autre.

Fournisseur de services électroniques
Personne qui fournit des biens ou des services dans le but de permettre à un dépositaire de renseignements sur la santé d'employer des moyens électroniques de recueillir, d'utiliser, de modifier, de divulguer, de conserver ou d'éliminer des renseignements personnels sur la santé et qui comprend un fournisseur de réseau d'information sur la santé.

Atteinte à la confidentialité
Atteinte à la confidentialité a la même signification que dans la *Politique sur la gestion des atteintes à la vie privée du dossier de santé électronique* et ses procédures connexes, telles que modifiées de temps à autre.

Atteinte à la sécurité
Atteinte à la sécurité a la même signification que dans la *Politique sur la gestion des incidents de sécurité relatifs aux renseignements du dossier de santé électronique* et ses procédures connexes, telles que modifiées de temps à autre.

Structure d'administration de la politique	Solution ConnexionOntario	Dépôt des Services communs d'imagerie diagnostique
Comité de protection de la vie privée et de sécurité	Protection de la vie privée : Comité de protection de la vie privée (Connecting	Protection de la vie privée : Groupe de travail sur la protection de la vie

[3] *Le Tableau 1 : Organismes de gestion appropriés* renvoie au comité de protection de la vie privée et de sécurité applicable et à l'organisme de surveillance applicable.

applicable	Privacy) Sécurité : Comité de sécurité (Connecting Security)	privée et la sécurité des Services communs d'imagerie diagnostique Sécurité : Comité de sécurité (Connecting Security)
Organisme de surveillance applicable	Protection de la vie privée : Comité directeur de ConnexionOntario Sécurité : Comité stratégique de cyberSanté Ontario	Protection de la vie privée : Comité exécutif des Services communs d'imagerie diagnostique Sécurité : Comité stratégique de cyberSanté Ontario

Tableau 1: Organisme de gouvernance applicable

Terme ou acronyme	Définition
DRS	Dépositaire de renseignements sur la santé
RPS	Renseignements personnels sur la santé, tel que le terme est défini dans la *Loi de 2004 sur la protection des renseignements personnels sur la santé*
LPRPS	*Loi de 2004 sur la protection des renseignements personnels sur la santé*
MS	Mandataire spécial tel que le définit la *Loi de 2004 sur la protection des renseignements personnels sur la santé*

7 Références et documents connexes

Loi de 2004 sur la protection des renseignements personnels sur la santé (LPRPS)
Politique de gestion du consentement relatif au dossier de santé électronique et ses procédures connexes
Politique de gestion des atteintes à la confidentialité du dossier de santé électronique et ses procédures connexes
Politique de conservation des dossiers électroniques de santé et ses procédures connexes
Politique sur la sécurité des renseignements du dossier de santé électronique et ses procédures connexes
Politique de gestion des incidents de sécurité relatifs aux renseignements du dossier de santé électronique et ses procédures connexes

eHealth Ontario

Politique sur la formation en protection de la confidentialité et de la sécurité

Dossier de santé électronique

Version : 1.2

N° de document : 3877

Ontario
eHealth Ontario

Gestion du document

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

Historique des approbations

APPROBATEURS	DATE D'APPROBATION
Membres du Comité ConnectingPrivacy	24 juin 2014

Historique des révisions

NUMÉRO DE VERSION	DATE AAAA-MM-JJ	Résumé des changements	AUTEUR DES CHANGEMENTS
1.0	2014-11-17	Version définitive	Urooj Kirmani, analyste principal en protection de la vie privée, cyberSanté Ontario
0.01	2014-11-04	Première version établie en fonction de la Politique harmonisée sur la formation en protection de la confidentialité et de la sécurité v. 1.0 du Comité ConnectingPrivacy.	Promila Gonsalves, analyste en protection de la vie privée, cyberSanté Ontario

1 Table des matières

1 Objectif

Définir les politiques, les procédures et les pratiques pour assurer que les mandataires et fournisseurs de services électroniques des dépositaires de renseignements sur la santé (DRS) et cyberSanté Ontario sont bien informés de leurs responsabilités en vertu de la LPRPS, des accords applicables en la matière et des politiques, des procédures et des pratiques en matière de protection de la confidentialité et de la sécurité mises en œuvre pour le dossier de santé électronique (DSE).

2 Portée

La présente politique et ses procédures connexes s'appliquent à la fourniture par les DRS et cyberSanté Ontario d'information à leurs mandataires et fournisseurs de services électroniques pour bien les informer de leurs responsabilités en vertu de la LPRPS, des accords applicables en la matière et des politiques, des procédures et des pratiques en matière de protection de la confidentialité et de la sécurité mises en œuvre pour le DSE. Le DSE est composé de la solution ConnexionOntario et du Dépôt du Service commun d'imagerie diagnostique. La solution ConnexionOntario et le Dépôt du service commun d'imagerie diagnostique sont le dépôt clinique ou des systèmes auxiliaires cliniques destinés à stocker et à rendre accessibles des renseignements personnels sur la santé (RPS) contenus dans les systèmes électroniques de renseignements sur la santé des dépositaires de ces renseignements[1].

La présente politique et ses procédures connexes ne s'appliquent pas à la formation en protection de la confidentialité et de la sécurité :

- pour tout système autre que le DSE;
- pour toute information autre que les renseignements personnels sur la santé (RPS) du DSE;
- pour les mandataires des DRS qui ne collectent, n'utilisent ni ne divulguent de RPS du DSE;
- pour les fournisseurs de services électroniques des DRS qui ne consultent, ne manipulent ni ne traitent autrement des RPS du DSE; ou
- pour les mandataires et fournisseurs de services électroniques de cyberSanté Ontario qui ne consultent, ne manipulent ni ne traitent autrement les RPS du DSE.

La présente politique et ses procédures connexes ne s'appliquent pas non plus à la formation de base en protection de la confidentialité et de la sécurité offerte par les DRS et cyberSanté Ontario à leurs mandataires et fournisseurs de services électroniques.

3 Politique

3.1 Fondements

3.1.1 La *Loi de 2004 sur la protection des renseignements personnels sur la santé* (LPRPS) exige que tout DRS autre qu'une personne naturelle, comme une société ou un partenariat, désigne une personne-ressource pour faciliter sa conformité à la LPRPS et assurer que tous ses mandataires sont bien informés de leurs responsabilités en vertu de cette Loi.

3.1.2 La LPRPS permet à tout DRS qui est une personne naturelle de désigner une personne-ressource pour faciliter sa conformité à la LPRPS et assurer que tous ses mandataires sont bien informés de leurs responsabilités en vertu de cette Loi. Tout DRS qui est une personne naturelle et qui ne désigne pas de personne-ressource pour exécuter ces fonctions, est tenu d'exécuter ces fonctions par ses propres moyens.

[1] Les divergences d'exigences de la politique et de la procédure entre la solution ConnexionOntario et le Dépôt du service commun d'imagerie diagnostique sont soulignées dans la politique.

3.1.3 La LPRPS exige que cyberSanté Ontario s'assure que les personnes qui agissent en son nom acceptent et respectent les conditions et restrictions nécessaires pour permettre à cyberSanté Ontario de se conformer à la LPRPS.

3.1.4 Les DRS et cyberSanté Ontario doivent avoir en place et maintenir les politiques, les procédures et les pratiques nécessaires en matière de confidentialité et de sécurité pour leur permettre de se conformer à leurs obligations en vertu de la LPRPS, des accords applicables en la matière et de la présente politique et de ses procédures connexes.

3.1.5 Les DRS et cyberSanté Ontario doivent avoir en place et maintenir des politiques, des procédures et des pratiques en matière de confidentialité et de sécurité qui se conforment à la LPRPS et sensibiliser leurs mandataires et leurs fournisseurs de services électroniques à ces politiques, ces procédures et ces pratiques comme l'exige la LPRPS.

3.1.6 Les DRS et cyberSanté Ontario prendront les mesures raisonnables dans les circonstances pour s'assurer que leurs mandataires et leurs fournisseurs de services électroniques se conforment à la LPRPS, aux accords applicables en la matière et à la présente politique et à ses procédures connexes.

4 Procédures

4.1 Procédure relative à la création par cyberSanté Ontario de matériel de formation en protection de la confidentialité et de la sécurité

4.1.1 cyberSanté Ontario élaborera et diffusera du matériel de formation en protection de la confidentialité et de la sécurité pour permettre aux DRS et à cyberSanté Ontario de former leurs mandataires et fournisseurs de services électroniques qui collectent, utilisent ou diffusent, des RPS du DSE ou qui consultent, manipulent ou traitent autrement les RPS du DSE, selon le cas, à leurs obligations et leurs responsabilités en matière de protection de la confidentialité et de la sécurité.

4.1.2 cyberSanté Ontario doit s'assurer que le matériel de formation en protection de la confidentialité et de la sécurité est fondé sur les rôles pour permettre aux DRS et aux mandataires et fournisseurs de services électroniques des DRS et de cyberSanté Ontario de comprendre et de remplir leurs obligations et responsabilités concernant le DSE dans leurs opérations quotidiennes.

4.1.3 Au minimum, le matériel de formation en protection de la confidentialité et de la sécurité doit inclure l'information décrite dans le paragraphe 4.4.1.

4.1.4 cyberSanté Ontario révisera et rafraîchira le matériel de formation en protection de la confidentialité et de la sécurité tous les deux ans ou avant lorsque des modifications de la LPRPS, des accords en la matière ou des politiques, des procédures et des pratiques en matière de protection de la confidentialité et de la sécurité mises en œuvre pour le DSE ont des répercussions sur les responsabilités et les obligations des DRS, de cyberSanté Ontario ou de leurs agents, ou des trois, et des fournisseurs de services électroniques concernant le DSE.

4.2 Procédure pour informer les mandataires et fournisseurs de services électroniques de leurs obligations en matière de protection de la confidentialité et de la sécurité

4.2.1 Les DRS doivent s'assurer que tous leurs mandataires et fournisseurs de services électroniques[2] sont bien informés de leurs responsabilités en vertu de la LPRPS, des accords en la matière et des politiques, des procédures et des pratiques relatives à la protection de la confidentialité et de la sécurité du DSE, avant de permettre à leurs mandataires et fournisseurs de services électroniques de collecter, d'utiliser ou de diffuser, ou de consulter, de manipuler ou de traiter autrement les RPS du DSE, selon le cas.

[2] Toute référence de la présente politique et de ses procédures connexes aux mandataires et fournisseurs de services électroniques d'un ou des DRS renvoie aux mandataires et fournisseurs de services électroniques autres que les mandataires ou fournisseurs de services électroniques de cyberSanté Ontario.

4.2.2 cyberSanté Ontario doit s'assurer que tous ses mandataires et des fournisseurs de services électroniques sont bien informés de leurs responsabilités en vertu de la LPRPS, des accords en la matière et des politiques, des procédures et des pratiques relatives à la protection de la confidentialité et de la sécurité du DSE, avant de permettre à ses mandataires et ses fournisseurs de services électroniques de consulter, de manipuler ou de traiter autrement les RPS du DSE, selon le cas.

4.2.3 Les DRS et cyberSanté Ontario ne permettront pas à leurs mandataires et leurs fournisseurs de services électroniques de continuer à collecter, utiliser ou diffuser ou à consulter, manipuler ou traiter autrement les RPS du DSE, selon le cas, à moins qu'ils aient été bien informés de leurs responsabilités pertinentes en vertu de la LPRPS, des accords applicables en la matière et des politiques, des procédures et des pratiques relatives à la protection de la confidentialité et de la sécurité mises en œuvre pour le DSE.

4.2.4 Les DRS et cyberSanté Ontario, quand ils informent leurs mandataires et leurs fournisseurs de services électroniques de leurs obligations en vertu de la LPRPS et des politiques, des procédures et des pratiques relatives à la protection de la confidentialité et de la sécurité mises en œuvre pour le DSE, s'assureront qu'ils sont mis au fait de l'information décrite dans le paragraphe 4.4.1, si elle est pertinente à leurs obligations quotidiennes.

4.2.5 Les DRS et cyberSanté Ontario imposeront des sanctions aux mandataires et aux fournisseurs de services électroniques qui ne comprennent pas leurs obligations pertinentes en vertu de la LPRPS, des accords applicables en la matière et des politiques, des procédures et des pratiques relatives à la protection de la confidentialité et de la sécurité mises en œuvre pour le DSE.

4.2.6 Les DRS et cyberSanté Ontario devront pouvoir montrer preuves à l'appui que leurs mandataires et leurs fournisseurs de services électroniques comprennent leurs obligations pertinentes en vertu de la LPRPS, des accords applicables en la matière et des politiques, des procédures et des pratiques relatives à la protection de la confidentialité et de la sécurité mises en œuvre pour le DSE.

4.3 Procédure relative aux accords de l'utilisateur final

4.3.1 cyberSanté Ontario s'assurera que le dossier de santé électronique exige des DRS, des mandataires et des fournisseurs de services électroniques des DRS et de cyberSanté Ontario qu'ils reconnaissent les responsabilités et les obligations de l'accord de l'utilisateur final et acceptent de s'y conformer avant de collecter, d'utiliser ou de diffuser, ou de consulter, manipuler ou traiter autrement les RPS du DSE, selon le cas, et au moins chaque année par la suite.

4.3.2 cyberSanté Ontario s'assurera que le dossier de santé électronique ne permet pas aux mandataires et fournisseurs de services électroniques des DRS et de cyberSanté Ontario de collecter, d'utiliser ou de diffuser, ou de consulter, de manipuler ou de traiter autrement les RPS du DSE, selon le cas, à moins qu'ils aient accepté de se conformer aux responsabilités et obligations de l'accord de l'utilisateur final annuel.

4.3.3 cyberSanté Ontario rédigera et mettra en œuvre un accord de l'utilisateur final qui, au minimum :

- établit les fins auxquelles on permet aux DRS et aux fournisseurs de services électroniques de collecter, d'utiliser ou de diffuser les RPS du DSE ou de les consulter, de les manipuler ou de les traiter autrement, selon le cas;
- établit les fins auxquelles on permet aux mandataires et fournisseurs de services électroniques de cyberSanté Ontario de consulter, de manipuler ou de traiter autrement les RPS du DSE;
- exige des DRS et des mandataires et fournisseurs de services électroniques des DRS et de cyberSanté Ontario qu'ils déclarent avoir lu, compris et accepté de se conformer aux politiques et aux pratiques relatives à la protection de la confidentialité et de la sécurité mises en œuvre pour le DSE;
- exige des DRS et des mandataires et fournisseurs de services électroniques des DRS et de cyberSanté Ontario qu'ils acceptent de se conformer à la LPRPS;
- exige des DRS et des mandataires et fournisseurs de services électroniques des DRS et de cyberSanté Ontario qu'ils mettent en œuvre les sauvegardes administratives, techniques et physiques établies dans l'accord de l'utilisateur final pour protéger les RPS du DSE;
- exige des DRS et des mandataires et fournisseurs de services électroniques des DRS et de cyberSanté Ontario qu'ils avisent conformément à la *Politique sur la gestion des atteintes à la confidentialité du dossier de santé électronique* et ses procédures connexes, telles que modifiées de temps à autre, ou à la *Politique sur la gestion des incidents de sécurité relatifs aux renseignements du dossier de santé électronique* et ses procédures connexes, telles que modifiées de temps à autre, selon le cas, de toute atteinte à la confidentialité des renseignements personnels sur la santé, réelle ou suspectée, qui s'est produite ou est sur le point de se produire en lien avec le DSE; et

- établit les conséquences de toute atteinte à l'accord de l'utilisateur final.

4.4 Contenu de la formation en protection de la confidentialité et de la sécurité

4.4.1 Pour informer les mandataires et fournisseurs de services électroniques des DRS et de cyberSanté Ontario de leurs responsabilités en vertu de la LPRPS, des accords applicables en la matière et des politiques, des procédures et des pratiques en matière de protection des renseignements personnels et de sécurité du DSE, l'information qui suit sera incluse lorsqu'elle est pertinente aux fonctions quotidiennes du mandataire ou du fournisseur de services électroniques :

- la nature des RPS conservés dans le DSE;
- le statut en vertu de la LPRPS de cyberSanté Ontario et des autres organismes qui participent au DSE et les responsabilités et obligations issues de ce statut;
- les fins auxquelles on permet aux DRS et à leurs mandataires et à leurs fournisseurs de services électroniques de collecter, d'utiliser ou de diffuser les RPS du DSE ou de les consulter, manipuler ou traiter autrement, selon le cas;
- le pouvoir des DRS et de leurs mandataires et de leurs fournisseurs de services électroniques de collecter, d'utiliser et de diffuser des RPS du DSE ou de les consulter, manipuler ou traiter autrement, selon le cas;
- les fins auxquelles on permet à cyberSanté Ontario et à ses mandataires et à ses fournisseurs de services électroniques de consulter, de manipuler ou de traiter autrement les RPS du DSE, et les limites qu'on leur impose en la matière;
- le pouvoir pour cyberSanté Ontario et ses mandataires et ses fournisseurs de services électroniques de consulter, de manipuler ou de traiter les RPS du DSE;
- une vue d'ensemble des politiques, des procédures et des pratiques en matière de protection de la confidentialité et de sécurité mises en œuvre pour le DSE, et les responsabilités et obligations des DRS et des mandataires et des fournisseurs de services électroniques des DRS et de cyberSanté Ontario issues de ces politiques, ces procédures et ces pratiques;
- les conséquences de toute atteinte aux politiques, aux procédures et aux pratiques en matière de protection de la confidentialité et de la sécurité mises en œuvre pour le DSE;
- les sauvegardes administratives, techniques et physiques mises en place pour protéger les RPS du DSE contre le vol, la perte ou l'utilisation ou la diffusion non autorisées et contre toute copie, modification ou élimination;
- les responsabilités et les obligations des DRS et des mandataires et des fournisseurs de services électroniques des DRS et de cyberSanté Ontario dans la mise en œuvre des sauvegardes administratives, techniques et physiques;
- l'accord de l'utilisateur final que les DRS et les mandataires et les fournisseurs de services électroniques des DRS et de cyberSanté Ontario doivent reconnaître et auquel ils doivent accepter de se conformer;
- les responsabilités et obligations des DRS et des mandataires et des fournisseurs de services électroniques des DRS et de cyberSanté Ontario relatives à la détection, la déclaration, au confinement et à la participation aux enquêtes et aux mesures correctrices prises contre les atteintes à la protection de la confidentialité et de la sécurité; et
- une déclaration informant les mandataires et les fournisseurs de services électroniques des DRS et de cyberSanté Ontario qu'ils sont assujettis à leurs obligations professionnelles en vertu de leur organisme de réglementation, le cas échéant.

5 Exécution[3]

5.1.1 Tous les cas de non-conformité seront examinés par le comité de protection de la vie privée et de sécurité applicable. Le comité de protection de la vie privée et de sécurité applicable recommandera les mesures appropriées à l'organisme de surveillance applicable.

5.1.2 L'organisme de surveillance pertinent a le pouvoir d'imposer les sanctions appropriées, jusqu'à et y compris la fin de l'accord en la matière avec le DRS ou la fin des privilèges d'accès des mandataires et des fournisseurs de services électroniques, et d'exiger la mise en œuvre de mesures correctrices.

6 Glossaire

Dossier de santé électronique (DSE)
Ensemble de la solution ConnexionOntario et du Dépôt du Service commun d'imagerie diagnostique, soit des dépôts ou des systèmes auxiliaires cliniques destinés à stocker et à rendre accessibles des renseignements personnels sur la santé contenus dans les systèmes électroniques de renseignements sur la santé des dépositaires de ces renseignements de manière à ne créer qu'un seul dépôt.

Fournisseur de services électroniques
Personne qui fournit des biens ou des services dans le but de permettre à un dépositaire de renseignements sur la santé d'employer des moyens électroniques de recueillir, d'utiliser, de modifier, de divulguer, de conserver ou d'éliminer des renseignements personnels sur la santé et qui comprend un fournisseur de réseau d'information sur la santé.

Accord de l'utilisateur final
Accord signé entre un DRS et les mandataires ou les fournisseurs de services électroniques d'un DRS et un accord signé entre cyberSanté Ontario et les mandataires et les fournisseurs de services électroniques de cyberSanté Ontario en matière de RPS.

Atteinte à la confidentialité
Atteinte à la confidentialité a la même signification que dans la *Politique sur la gestion des atteintes à la confidentialité du dossier de santé électronique* et ses procédures connexes, telles que modifiées de temps à autre.

Atteinte à la sécurité
Atteinte à la sécurité a le même sens que dans la *Politique de gestion des atteintes à la sécurité des renseignements du dossier de santé électronique* ainsi que ses procédures connexes, ce qui comprend les modifications qui y sont apportées de temps à autre.

Structure d'administration de la politique	Solution ConnexionOntario	Dépôt des Services communs d'imagerie diagnostique
Comité de protection de la vie privée et de sécurité applicable	Protection de la vie privée : Comité de protection de la vie privée (Connecting Privacy) Sécurité : Comité de sécurité (Connecting Security)	Protection de la vie privée : Groupe de travail sur la protection de la vie privée et la sécurité des Services communs d'imagerie diagnostique Sécurité : Comité de sécurité (Connecting Security)
Organisme de surveillance applicable	Protection de la vie privée : Comité directeur de ConnexionOntario	Protection de la vie privée : Comité exécutif des Services communs d'imagerie diagnostique

[3] *Le Tableau 1 : Organismes de gestion appropriés* renvoie au comité de protection de la vie privée et de sécurité applicable et à l'organisme de surveillance applicable.

	Sécurité : Comité stratégique de cyberSanté Ontario	Sécurité : Comité stratégique de cyberSanté Ontario

Tableau 1: Organisme de gouvernance applicable

Terme ou acronyme	Définition
DRS	Dépositaire de renseignements sur la santé
RPS	Renseignements personnels sur la santé, tel que le terme est défini dans la *Loi de 2004 sur la protection des renseignements personnels sur la santé*
LPRPS	*Loi de 2004 sur la protection des renseignements personnels sur la santé*

7 Références et documents connexes

Loi de 2004 sur la protection des renseignements personnels sur la santé (LPRPS)
Politique de gestion des atteintes à la confidentialité du dossier de santé électronique et ses procédures connexes
Politique de gestion des atteintes à la sécurité des renseignements du dossier de santé électronique

eHealth Ontario

Politique de gestion des atteintes à la confidentialité

Dossier de santé électronique

Version : 2.0

Nº de document : 3872

Ontario
eHealth Ontario

Gestion du document

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

Historique des approbations

APPROBATEURS	DATE D'APPROBATION
Membres du Comité ConnectingPrivacy	6 juillet 2016

Historique des révisions

NUMÉRO DE VERSION	DATE	Résumé des changements	AUTEUR DES CHANGEMENTS
2.0	2016-12-01	Révisions conformément à l'évaluation des politiques par le CPC	Rand Muhtam, analyste en protection de la vie privée, cyberSanté Ontario
1.1	2015-11-25	Révisions mineures – mise à jour pour ConnexionOntario	Samara Strub, analyste en protection de la vie privée, cyberSanté Ontario
1.0	2014-11-17	Version définitive	Urooj Kirmani, analyste principal en protection de la vie privée, cyberSanté Ontario
0.01	2014-11-04	Première version établie en fonction de la Politique harmonisée sur la gestion des atteintes à confidentialité 1.4 du Comité ConnectingPrivacy.	Promila Gonsalves, analyste en protection de la vie privée, cyberSanté Ontario

Table des matières

1 Objectif

Définir les politiques, les procédures et les pratiques qui s'appliquent à la détection, la déclaration, le confinement, la notification, l'enquête et la correction relatifs aux atteintes à la confidentialité du dossier de santé électronique (DSE).

2 Portée

La présente politique et ses procédures connexes s'appliquent aux atteintes à la confidentialité du DSE et non à tout système autre que le DSE ou à toute information autre que les renseignements personnels sur la santé (RPS) du DSE. Le DSE est composé de la solution ConnexionOntario et du Dépôt des Services communs d'imagerie diagnostique. La solution ConnexionOntario et le Dépôt des Services communs d'imagerie diagnostique sont le dépôt clinique ou des systèmes auxiliaires cliniques destinés à stocker et à rendre accessibles des renseignements personnels sur la santé (RPS) contenus dans les systèmes électroniques de renseignements sur la santé des dépositaires de ces renseignements[1].

3 Politique

3.1 Fondements

3.1.1 La *Loi de 2004 sur la protection des renseignements personnels sur la santé* (LPRPS) exige que les dépositaires de renseignements sur la santé (DRS) prennent des mesures raisonnables dans les circonstances pour garantir que les RPS sous leur garde ou leur contrôle sont protégés contre le vol, la perte, et l'utilisation ou la diffusion non autorisées et pour garantir que les dossiers de RPS sont protégés contre la copie, la modification ou l'élimination.

3.1.2 La LPRPS exige des DRS qu'ils s'assurent que les dossiers de RPS sous leur garde ou leur contrôle soient conservés, transférés et éliminés d'une façon sûre.

3.1.3 La LPRPS exige que tout mandataire d'un DRS l'avise à la première occasion raisonnable si les renseignements personnels sur la santé qu'il a manipulés au nom du DRS sont volés, perdus ou consultés par des personnes non autorisées.

3.1.4 En vertu de la LPRPS, cyberSanté Ontario doit à la première occasion aviser les DRS si cyberSanté Ontario ou ses mandataires et fournisseurs de services électroniques ont consulté, manipulé ou traité autrement les RPS en infraction à la LPRPS ou si ces renseignements personnels sur la santé ont été volés, perdus ou consultés par des personnes non autorisées.

3.1.5 En vertu de la LPRPS, les DRS doivent à la première occasion aviser les personnes dont les RPS ont été volés, perdus ou consultés par des personnes non autorisées.

3.1.6 La présente politique et ses procédures connexes permettront aux DRS et à cyberSanté Ontario de remplir leurs obligations en vertu de la LPRPS en ce qui trait à la détection, la déclaration, le confinement, la notification, l'enquête et la rectification de toute atteinte à la confidentialité du DSE.

3.1.7 Les DRS et cyberSanté Ontario doivent avoir en place et maintenir les politiques, les procédures et les pratiques nécessaires en matière de confidentialité et de sécurité pour leur permettre de se conformer à leurs obligations en vertu de la LPRPS, des accords applicables en la matière et de la présente politique et de ses procédures connexes.

---

[1] Les divergences d'exigences de la politique et de la procédure entre la solution ConnexionOntario et le Dépôt des Services communs d'imagerie diagnostique sont soulignées dans la politique.

3.1.8 Les DRS et cyberSanté Ontario prendront les mesures raisonnables dans les circonstances pour s'assurer que leurs mandataires et leurs fournisseurs de services électroniques se conforment à la LPRPS, aux accords applicables en la matière et à la présente politique et à ses procédures connexes.

3.1.9 cyberSanté Ontario devra avoir en place un programme pour permettre à cyberSanté Ontario et aux DRS de s'acquitter de leurs responsabilités en matière d'atteintes à la confidentialité du DSE conformément à la LPRPS, aux accords applicables en la matière et à la présente politique et à ses procédures connexes.

3.1.10 Les DRS et cyberSanté Ontario doivent avoir en place et maintenir des politiques, des procédures et des pratiques en matière de confidentialité et de sécurité qui se conforment à la LPRPS et sensibiliser leurs mandataires et leurs fournisseurs de services électroniques à ces politiques, ces procédures et ces pratiques comme l'exige la LPRPS.

4 Procédures

4.1 Procédure de détection des atteintes à la confidentialité

4.1.1 Les DRS et cyberSanté Ontario créeront et mettront en œuvre des politiques, des procédures et des pratiques pour recevoir les plaintes relatives aux atteintes à la confidentialité réelles ou suspectées du DSE qui leur permettent de se conformer à la LPRPS et à la *Politique sur les demandes de renseignements et les plaintes relatives au dossier de santé électronique* et ses procédures connexes, telles que modifiées de temps à autre.

4.1.2 Les DRS et cyberSanté Ontario créeront et mettront en œuvre des politiques, des procédures et des pratiques pour vérifier et surveiller toute atteinte réelle ou suspectée à la confidentialité du DSE qui se conforment à la LPRPS et à la *Politique sur la journalisation et la surveillance du dossier de santé électronique* et ses procédures connexes, telles que modifiées de temps à autre.

4.1.3 Les DRS s'assureront que leurs mandataires et fournisseurs de services électroniques les avisent, à la première occasion, de toute atteinte à la confidentialité, réelle ou suspectée, conformément à leurs politiques, à leurs procédures et à leurs pratiques internes et à la LPRPS.

4.1.4 cyberSanté Ontario s'assurera que ses mandataires et ses fournisseurs de services électroniques l'avisent, à la première occasion raisonnable, de toute atteinte à la confidentialité, réelle ou suspectée, conformément à ses politiques, ses procédures et ses pratiques internes et à la LPRPS.

4.1.5 Un DRS déclarera toute atteinte à la confidentialité, réelle ou suspectée, à cyberSanté Ontario aussitôt que possible, mais au plus tard avant la fin du jour ouvrable suivant la découverte de cette atteinte par la personne du DRS responsable de déclarer les atteintes à la confidentialité causées ou aggravées par :

- un autre DRS ou un mandataire ou un fournisseur de services électroniques d'un autre DRS;
- plus d'un DRS ou mandataire ou fournisseur de services électroniques de plus d'un DRS;
- cyberSanté Ontario ou un mandataire ou fournisseur de services électroniques de cyberSanté Ontario; ou
- toute personne non autorisée qui n'est pas un mandataire ou un fournisseur de services électroniques de cyberSanté Ontario ou d'un autre DRS.

4.1.6 À la réception d'un rapport en vertu du paragraphe 4.1.5 ou en cas de détection d'une atteinte à la confidentialité, réelle ou suspectée, cyberSanté Ontario devra, le plus tôt possible ou en tout cas au plus tard à la fin du jour ouvrable suivant sa détection ou sa déclaration, selon le cas, déclarer l'atteinte à la confidentialité réelle ou suspectée à chacun des DRS dont les mandataires ou les fournisseurs de services électroniques ont causé l'atteinte réelle ou suspectée ou y ont contribué, le cas échéant.

4.1.7 Tout rapport en vertu des paragraphes 4.1.5 et 4.1.6 contiendra tous les renseignements connus qui peuvent aider à déterminer s'il y a eu ou non atteinte à la confidentialité.

4.2 Procédure pour les atteintes à la confidentialité uniquement causées par un DRS qui a seul créé et contribué à créer les RPS du DSE

4.2.1 Dans le cas des atteintes à la confidentialité actuelles ou réelles causées seulement par un DRS ou par un mandataire ou un fournisseur de services électroniques d'un DRS[2] et que ce dernier a seulement créé et contribué à créer les RPS du DSE, le DRS devra, le plus tôt possible, déterminer s'il y a eu ou non atteinte à la confidentialité.

4.2.2 Tout DRS qui a déterminé qu'il s'est en effet produit une atteinte à la confidentialité ou qui a des motifs raisonnables de soupçonner une atteinte à la confidentialité devra :

- déclarer cette atteinte à la confidentialité à cyberSanté Ontario conformément au paragraphe 4.2.3 le plus tôt possible, mais en tout cas avant la fin du jour ouvrable suivant le jour où il a déterminé que l'atteinte s'est bien produite; et
- suivre ses politiques, ses procédures et ses pratiques internes pour aviser, à la première occasion raisonnable, la ou les personnes que les renseignements personnels sur la santé concernent conformément à la LPRPS et pour confiner, faire enquête et corriger l'atteinte à la confidentialité.

4.2.3 Dans sa déclaration de toute atteinte à la confidentialité à cyberSanté Ontario, le DRS devra fournir toute l'information connue au moment de la déclaration, y compris :

- une reconnaissance que le DRS a seul créé et contribué à créer les renseignements personnels sur la santé du DSE qui ont fait l'objet de l'atteinte à la confidentialité;
- une reconnaissance que le DRS, ses mandataires ou ses fournisseurs de services électroniques ont seuls causés cette atteinte à la confidentialité;
- le nom de chaque mandataire et de chaque fournisseur de services électroniques du DRS qui a seul causé l'atteinte à la confidentialité, lorsque le DRS qui a seul causé l'atteinte à la confidentialité juge ce nom pertinent (p. ex., collecte, utilisation ou diffusion intentionnelle des RPS par un mandataire);
- la date et l'heure de l'atteinte à la confidentialité;
- une description de la nature, de la portée et de la cause de l'atteinte à la confidentialité;
- une description des renseignements du DSE qui ont fait l'objet de l'atteinte à la confidentialité, sans divulguer aucun renseignement personnel sur la santé;
- les mesures prises pour confiner l'atteinte à la confidentialité;
- les mesures prises ou qui seront mises en œuvre pour corriger l'atteinte à la confidentialité et pour éviter qu'une atteinte semblable se reproduise à l'avenir; et
- le calendrier et les personnes responsables de la mise en œuvre des mesures pour corriger l'atteinte à la confidentialité et pour éviter qu'une atteinte semblable se reproduise à l'avenir.

4.2.4 Le plus tôt possible après l'enquête faite sur l'atteinte à la confidentialité, le DRS fournira à cyberSanté Ontario et à la ou aux personnes que les renseignements personnels sur la santé du DSE concernent :

- un résumé des résultats de l'enquête; et
- les mesures, connues à ce moment, qui ont été ou seront prises pour corriger l'atteinte à la confidentialité et pour prévenir toute atteinte à la confidentialité semblable à l'avenir conformément à ses politiques, ses procédures et ses pratiques internes.

4.3 Procédure pour les atteintes à la confidentialité seulement causées par un DRS qui n'a pas seul créé et contribué à créer les RPS du DSE

[2] Toute référence de la présente politique et de ses procédures connexes aux mandataires et aux fournisseurs de services électroniques d'un ou des DRS renvoie aux mandataires et fournisseurs de services électroniques autres que les mandataires et fournisseurs de services électroniques de cyberSanté Ontario.

Déterminer s'il y a ou non eu atteinte à la confidentialité

4.3.1 Dans le cas des atteintes à la confidentialité réelles ou suspectées causées seulement par un DRS ou des mandataires ou des fournisseurs de services électroniques d'un DRS et que ce dernier n'a pas seul créé et contribué à créer les RPS du dossier de santé électronique, le DRS ou le DRS dont les mandataires et les fournisseurs de services électroniques ont seuls causés l'atteinte à la confidentialité devront, le plus tôt possible après sa déclaration, déterminer si l'atteinte à la confidentialité est réelle ou suspectée.

Confinement

4.3.2 Lorsque le DRS ou le DRS dont les mandataires ou les fournisseurs de services électroniques ont seuls causé l'atteinte à la confidentialité a déterminé que l'atteinte est réelle, le DRS devra suivre ses propres politiques, procédures et pratiques internes pour confiner l'atteinte à la confidentialité et, le cas échéant, demander l'aide de cybersanté Ontario ou des autres DRS, ou des deux, en vertu du paragraphe 4.3.3 pour confiner l'atteinte à la confidentialité.

Déclaration à cyberSanté Ontario et aux DRS qui ont créé et contribué à créer les RPS du DSE

4.3.3 Lorsque le DRS ou le DRS dont les mandataires ou les fournisseurs de services électroniques ont seuls causé l'atteinte à la confidentialité a conclu que l'atteinte est réelle ou a des motifs raisonnables de soupçonner une atteinte à la confidentialité, le DRS devra déclarer l'atteinte à cyberSanté Ontario le plus tôt possible, mais en tout cas au plus tard avant la fin du jour ouvrable suivant cette conclusion. Dans sa déclaration de l'atteinte à la confidentialité, le DRS devra fournir toute l'information connue au moment de la déclaration, y compris :

- une reconnaissance que le DRS, ses mandataires ou ses fournisseurs de services électroniques ont seuls causé cette atteinte à la confidentialité;
- le nom de chaque mandataire et de chaque fournisseur de services électroniques du DRS qui a seul causé l'atteinte à la confidentialité, lorsque le DRS qui a seul causé l'atteinte à la confidentialité juge ce nom pertinent (p. ex., collecte, utilisation ou diffusion intentionnelle des RPS par un mandataire);
- une reconnaissance que les renseignements personnels sur la santé du DSE qui ont fait l'objet de l'atteinte à la confidentialité n'ont pas seulement été créés et ajoutés par le DRS;
- le nom de chaque DRS qui a créé et contribué à créer les renseignements personnels sur la santé du DSE;
- la date et l'heure de l'atteinte à la confidentialité;
- une description de la nature, de la portée et de la cause de l'atteinte à la confidentialité;
- une description des renseignements personnels sur la santé du DSE qui ont fait l'objet de l'atteinte à la confidentialité;
- la ou les personnes que concernent les RPS du DSE;
- les mesures prises pour confiner l'atteinte à la confidentialité;
- toute demande d'aide de cyberSanté Ontario ou des DRS, ou des deux, pour confiner l'atteinte à la confidentialité; et
- suffisamment d'information pour permettre d'aviser la ou les personnes que ces RPS concernent conformément à la LPRPS.

4.3.4 Le plus tôt possible, mais en tout cas au plus tard à la fin du jour ouvrable suivant la réception du rapport en vertu du paragraphe 4.3.3, cyberSanté Ontario devra déclarer l'atteinte à la confidentialité à chaque DRS qui a créé ou contribué à créer les RPS et devra les aviser :

- si le DRS a seul créé ou contribué à créer les renseignements personnels sur la santé du DSE qui ont fait l'objet de l'atteinte à la confidentialité;
- le nom de chacun des dépositaires de renseignements sur la santé qui a créé et contribué à créer les RPS du DSE qui ont fait l'objet de l'atteinte à la confidentialité s'il y en a plus d'un;
- le nom du DRS ou du DRS dont les mandataires et les fournisseurs de services électroniques ont seuls causé l'atteinte à la confidentialité;
- le nom de chaque mandataire et de chaque fournisseur de services électroniques du DRS qui a seul causé l'atteinte à la confidentialité, lorsque le DRS qui a seul causé l'atteinte à la confidentialité juge ce nom pertinent (p. ex., collecte, utilisation ou diffusion intentionnelle des RPS par un mandataire);

- la date et l'heure de l'atteinte à la confidentialité;
- une description de la nature, de la portée et de la cause de l'atteinte à la confidentialité;
- une description des renseignements personnels sur la santé du DSE qui ont fait l'objet de l'atteinte à la confidentialité;
- la ou les personnes que concernent les RPS du DSE;
- les mesures prises pour confiner l'atteinte à la confidentialité;
- toute aide qu'on demande au DRS de fournir pour confiner l'atteinte à la confidentialité; et
- suffisamment d'information pour permettre d'aviser la ou les personnes que ces RPS concernent conformément à la LPRPS.

4.3.5 cyberSanté Ontario et les autres DRS fourniront de l'assistance dans le confinement de l'atteinte à la confidentialité lorsque le DRS ou un DRS dont les mandataires et fournisseurs de services électroniques qui ont causé seuls l'atteinte à la confidentialité leur demande de le faire.

4.3.6 Le DRS ou un DRS dont les mandataires et fournisseurs de services électroniques qui ont causé seuls l'atteinte à la confidentialité déterminera également si l'atteinte à la confidentialité doit être déclarée à toute autre personne, y compris au Commissaire à l'information et à la protection de la vie privée/Ontario, aux organismes d'exécution de la loi ou de réglementation conformément à leurs politiques, leurs procédures et leurs pratiques internes.

Notification de la personne

4.3.7 Lorsque les renseignements personnels sur la santé du DSE qui ont fait l'objet de l'atteinte à la confidentialité ont été créés ou ajoutés par un autre DRS, ce dernier dépositaire de renseignements sur la santé (DRS) suivra ses politiques, ses procédures et ses pratiques internes pour aviser à la première occasion raisonnable la ou les personnes que les RPS concernent conformément à la LPRPS et au paragraphe 4.3.10.

4.3.8 Lorsque les RPS du dossier de santé électronique qui ont fait l'objet de l'atteinte à la confidentialité ont été créés ou ajoutés par plus d'un DRS, ces DRS désigneront le plus tôt possible, mais au plus tard 7 jours après la réception de l'information du paragraphe 4.3.4, le dépositaire de renseignements sur la santé qui sera responsable d'aviser la ou les personnes que ces DSE concernent conformément à la LPRPS et au paragraphe 4.3.10.

4.3.9 Pour désigner le DRS qui sera responsable d'aviser ces personnes, on tiendra compte :

- du DRS ou du DRS dont les mandataires et fournisseurs de services électroniques ont seuls causé l'atteinte à la confidentialité;
- du DRS de qui la ou les personnes ont reçu les soins de santé les plus récents; et
- du DRS de qui la ou les personnes ont reçu le plus de soins de santé.

4.3.10 Pour aviser la ou les personnes, le DRS du paragraphe 4.3.7 ou 4.3.8, selon le cas, devra au minimum lui ou leur fournir l'information qui suit :

- le nom du DRS ou du DRS dont les mandataires et les fournisseurs de services électroniques ont seuls causé l'atteinte à la confidentialité;
- le nom de chaque mandataire et de chaque fournisseur de services électroniques du DRS qui a seul causé l'atteinte à la confidentialité, lorsque le DRS qui a seul causé l'atteinte à la confidentialité juge ce nom pertinent (p. ex., collecte, utilisation ou diffusion intentionnelle des RPS par un mandataire);
- le nom de chaque DRS qui a créé et contribué à créer les renseignements personnels sur la santé du DSE;
- la date et l'heure de l'atteinte à la confidentialité;
- une description de la nature, de la portée et de la cause de l'atteinte à la confidentialité;
- une description des renseignements personnels sur la santé du DSE qui ont fait l'objet de l'atteinte à la confidentialité;
- les mesures prises pour confiner l'atteinte à la confidentialité;
- le nom de la personne responsable de l'enquête sur l'atteinte;

- Le DRS du paragraphe 4.3.7 ou 4.3.8 selon le cas, devra, le plus tôt possible après la réception du rapport écrit approuvé par cyberSanté Ontario, fournir aux personnes le résumé des résultats de l'enquête et les mesures, connues à ce moment-là, qui ont été ou seront prises pour corriger l'atteinte à la confidentialité et pour éviter toute atteinte semblable à l'avenir le plus tôt possible après la réception du rapport écrit approuvé par cyberSanté Ontario en vertu du paragraphe 4.3.29;
- les mesures que la ou les personnes peuvent prendre pour protéger leurs renseignements personnels ou pour minimiser les répercussions de l'atteinte à la confidentialité, le cas échéant;
- les nom et coordonnées du DRS du paragraphe 4.3.7 ou 4.3.8, selon le cas, à qui la ou les personnes peuvent adresser leurs demandes de renseignements et leurs préoccupations; et
- l'information concernant la manière de porter plainte au Commissaire à l'information et à la protection de la vie privée/Ontario.

4.3.11 cyberSanté Ontario et les autres DRS aideront à aviser la ou les personnes que les RPS concernent lorsque le DRS leur demande de le faire dans le paragraphe 4.3.7 ou 4.3.8, selon le cas.

Enquête

4.3.12 cyberSanté Ontario, le ou les DRS qui ont créé et contribué à créer les RPS du DSE qui ont fait l'objet de l'atteinte à la confidentialité ou le DRS dont les mandataires et fournisseurs de services électroniques ont seuls causé l'atteinte à la confidentialité devront, le plus tôt possible, mais au plus tard 7 jours après avoir déterminé qu'il y a bien eu atteinte à la confidentialité, désigner un enquêteur pour cette atteinte.

4.3.13 Pour désigner l'enquêteur pour cette atteinte en vertu du paragraphe 4.3.12, il faut :

- savoir si le DRS ou le DRS dont les mandataires et fournisseurs de services électroniques ont seuls causé l'atteinte à la confidentialité a la capacité de faire enquête sur l'atteinte; et
- si un autre DRS ou cyberSanté Ontario seraient mieux à même de faire enquête sur cette atteinte.

4.3.14 L'enquêteur de l'atteinte à la confidentialité devra, le plus tôt possible, mais pas plus tard que 7 jours après qu'on ait déterminé qu'il y a bien eu atteinte à la confidentialité, faire enquête sur cette atteinte conformément aux politiques, aux procédures et aux pratiques internes et au paragraphe 4.3.15.

4.3.15 Dans la conduite de l'enquête, l'enquêteur devra consulter le DRS ou le DRS dont les mandataires et les fournisseurs de services électroniques ont seuls causé l'atteinte, lorsque le DRS n'est pas l'enquêteur de cette atteinte, et devra :

- déterminer la nature, la portée et la cause de l'atteinte à la confidentialité;
- s'assurer que l'atteinte à la confidentialité a été confinée efficacement ou déterminer s'il faut prendre d'autres mesures pour la confiner;
- évaluer la pertinence des sauvegardes administratives, techniques et physiques;
- déterminer quelles mesures doivent être prises pour corriger l'atteinte à la confidentialité et pour éviter toute atteinte à la confidentialité semblable à l'avenir; et
- déterminer le calendrier et les personnes responsables de la mise en œuvre des mesures pour corriger l'atteinte à la confidentialité et pour éviter toute atteinte à la confidentialité semblable à l'avenir.

4.3.16 Les autres DRS et cyberSanté Ontario, lorsqu'ils ne sont pas responsables de l'enquête sur l'atteinte à la confidentialité, devront fournir de l'aide pour l'enquête lorsque l'enquêteur le leur demande.

4.3.17 Des rapports d'étapes pour l'enquête seront fournis par l'enquêteur lorsque cyberSanté Ontario, le DRS ou les DRS qui ont créé et contribué à créer les RPS du DSE qui ont fait l'objet de l'atteinte à la confidentialité ou le DRS ou le DRS dont les mandataires et les fournisseurs de services électroniques ont seuls causé l'atteinte à la confidentialité et qu'ils ne sont pas responsables de l'enquête, le leur demande.

4.3.18 Le plus tôt possible, mais au plus tard 7 jours après l'achèvement de l'enquête, l'enquêteur de l'atteinte à la confidentialité préparera un rapport écrit qui, au minimum, contienne l'information suivante :

- le DRS ou le DRS dont les mandataires et fournisseurs de services électroniques ont seuls causé l'atteinte à la confidentialité;

- le nom de chaque mandataire et de chaque fournisseur de services électroniques du DRS qui a seul causé l'atteinte à la confidentialité, lorsque le DRS qui a seul causé l'atteinte à la confidentialité juge ce nom pertinent (p. ex., collecte, utilisation ou diffusion intentionnelle des RPS par un mandataire);
- le nom de chaque DRS qui a créé et contribué à créer les RPS du DSE;
- la date et l'heure de l'atteinte à la confidentialité;
- la nature, la portée et la cause de l'atteinte à la confidentialité;
- une description des renseignements du DSE qui ont fait l'objet de l'atteinte à la confidentialité, sans divulguer aucun renseignement personnel sur la santé;
- les personnes à qui l'atteinte à la confidentialité a été déclarée en vertu du paragraphe 4.3.6;
- les mesures prises pour confiner l'atteinte à la confidentialité;
- la nature, la portée et le processus d'enquête sur l'atteinte à la confidentialité;
- les mesures qu'on recommande pour corriger l'atteinte à la confidentialité et pour éviter qu'une atteinte semblable se reproduise à l'avenir; et
- le calendrier et les personnes responsables proposées pour la mise en œuvre des mesures pour corriger l'atteinte à la confidentialité et pour éviter qu'une atteinte semblable se reproduise à l'avenir.

4.3.19 Le plus tôt possible, mais au plus tard 4 jours après l'achèvement du rapport écrit du paragraphe 4.3.18, l'enquêteur responsable de l'atteinte à la confidentialité fournira, aux fins d'examen et de commentaire, un rapport écrit au DRS ou au DRS dont les mandataires et les fournisseurs de services électroniques ont seuls causé l'atteinte, lorsque le DRS n'est pas responsable d'effectuer l'enquête.

4.3.20 Le DRS qui a reçu le rapport écrit en vertu du paragraphe 4.3.19 devra, le plus tôt possible, mais au plus tard 7 jours après l'avoir reçu, l'examiner et faire des commentaires à l'enquêteur responsable de l'enquête. Si aucun commentaire n'est fourni dans les 7 jours après réception, on tiendra pour acquis qu'il n'y a pas de commentaires.

4.3.21 Le responsable de l'enquête sur l'atteinte à la confidentialité devra, le plus tôt possible, mais au plus tard 7 jours après réception des commentaires en vertu du paragraphe 4.3.20, faire les modifications requises et fournir un rapport écrit à cyberSanté Ontario lorsque ce dernier n'est pas chargé de l'enquête.

4.3.22 Lorsque cyberSanté Ontario n'est pas chargé de l'enquête, il devra, le plus tôt possible, mais au plus tard 7 jours après l'avoir reçu en vertu du paragraphe 4.3.21, examiner et faire des commentaires sur le rapport écrit.

4.3.23 Le plus tôt possible, mais au plus tard 7 jours après avoir reçu ou préparé le rapport écrit du paragraphe 4.3.21, selon le cas, cyberSanté Ontario transférera le rapport écrit avec ses commentaires, le cas échéant, au DRS ou au DRS qui a créé et contribué à créer les RPS du DSE qui a fait l'objet de l'atteinte à la confidentialité aux fins d'examen et de commentaire.

4.3.24 Le ou les DRS qui ont reçu le rapport écrit en vertu du paragraphe 4.3.23 devront, le plus tôt possible, mais au plus tard 7 jours après l'avoir reçu, l'examiner et faire des commentaires à cyberSanté Ontario. Si aucun commentaire n'est fourni dans les 7 jours après réception, on tiendra pour acquis qu'il n'y a pas de commentaires.

4.3.25 cyberSanté Ontario devra, le plus tôt possible, mais au plus tard 4 jours après avoir reçu les commentaires en vertu du paragraphe 4.3.24, aviser l'enquêteur, lorsque cyberSanté Ontario n'est pas chargé de l'enquête, de toute modification qui doit être apportée au rapport écrit ou toute mesure supplémentaire qui doit être prise pour confiner, ou corriger l'atteinte à la confidentialité ou pour en faire l'enquête, le cas échéant.

4.3.26 Le responsable de l'enquête devra, le plus tôt possible, mais au plus tard 7 jours après avoir reçu les commentaires en vertu du paragraphe 4.3.24 ou 4.3.25, selon le cas, apporter les modifications et prendre les mesures supplémentaires pour confiner, corriger l'atteinte à la confidentialité ou en faire l'enquête en consultation avec le DRS ou le DRS dont les mandataires et les fournisseurs de services électroniques ont seuls causé l'atteinte à la confidentialité, lorsque le DRS n'est pas chargé de l'enquête, et préparer un rapport écrit révisé.

4.3.27 Lorsque cyberSanté Ontario n'est pas chargé de l'enquête, l'enquêteur qui en est chargé devra, le plus tôt possible, mais au plus tard 7 jours après avoir reçu les commentaires en vertu du paragraphe 4.3.25, fournir le rapport écrit révisé à cyberSanté Ontario.

4.3.27.1 Le plus tôt possible, mais au plus tard 4 jours après avoir reçu ou préparé le rapport écrit révisé des paragraphes 4.3.26 ou 4.3.27, selon le cas, cyberSanté Ontario transférera le rapport écrit révisé au comité de protection de la vie privée et de sécurité applicable aux fins d'examen et d'approbation et, par la suite, à l'organisme de surveillance applicable aux fins d'examen et d'approbation.

4.3.27.2 Le plus tôt possible, mais au plus tard 4 jours après avoir reçu l'approbation du rapport écrit de l'organisme de surveillance applicable, cyberSanté Ontario transférera le rapport écrit approuvé au DRS ou au DRS dont les mandataires et les fournisseurs de services électroniques ont seuls causé l'atteinte à la confidentialité, à chaque DRS qui a créé ou contribué à créer les RPS du DSE qui ont fait l'objet de l'atteinte et à chaque DRS responsable de la mise en œuvre des mesures pour corriger ou pour éviter toute atteinte à la confidentialité semblable à l'avenir.

4.3.28 Le DRS des paragraphes 4.3.7 ou 4.3.8, selon le cas, devra fournir à la ou aux personnes que concernent les renseignements personnels sur la santé du DSE le plus tôt possible après la réception du rapport de cyberSanté Ontario en vertu du paragraphe 4.3.29 :

- un résumé des résultats de l'enquête; et
- les mesures, connues à ce moment, qui ont été ou seront prises pour corriger l'atteinte à la confidentialité et pour prévenir toute atteinte à la confidentialité semblable à l'avenir conformément à ses politiques, ses procédures et ses pratiques internes.

4.4 Procédure pour toute atteinte à la confidentialité à laquelle plus d'un DRS ont contribué

Déterminer s'il y a ou non eu atteinte à la confidentialité

4.4.1 Lorsque plus d'un DRS ou que les mandataires et les fournisseurs de services électroniques de plus d'un DRS ont causé une atteinte à la confidentialité ou y ont contribué, ils devront, le plus tôt possible, mais au plus tard à la fin du jour ouvrable après la déclaration de l'atteinte à la confidentialité, désigner le DRS responsable de déterminer s'il y a eu atteinte et d'en assurer le confinement.

4.4.2 Le DRS désigné en vertu du paragraphe 4.4.1 devra, le plus tôt possible, déterminer s'il y a eu atteinte à la confidentialité.

Confinement

4.4.3 Lorsque le DRS désigné en vertu du paragraphe 4.4.1 a déterminé qu'il y a bien eu atteinte à la confidentialité, le DRS devra suivre ses politiques, ses procédures et ses pratiques internes pour confiner l'atteinte à la confidentialité et, le cas échéant, demander l'aide de cybersanté Ontario ou des autres DRS, ou des deux, en vertu du paragraphe 4.4.4 pour confiner l'atteinte à la confidentialité.

Déclaration à cyberSanté Ontario et aux DRS qui ont créé et contribué à créer les RPS du DSE

4.4.4 Lorsque le DRS désigné en vertu du paragraphe 4.4.1 a déterminé qu'il y a eu atteinte à la confidentialité ou a des motifs raisonnables de soupçonner une atteinte à la confidentialité, il devra, en consultation avec les autres DRS et les autres DRS dont les mandataires ou les fournisseurs de services électroniques ont causé l'atteinte à la confidentialité ou y ont contribué, déclarer l'atteinte en question à cyberSanté Ontario le plus tôt possible, mais au plus tard avant la fin du jour ouvrable suivant cette détermination. Dans sa déclaration de toute atteinte à la confidentialité, le DRS désigné en vertu du paragraphe 4.4.1 devra fournir toute l'information connue au moment de la déclaration, y compris :

- le nom de chaque DRS ou de chaque DRS dont les mandataires et les fournisseurs de services électroniques ont causé l'atteinte à la confidentialité ou y ont contribué;
- le nom de chaque mandataire et fournisseur de services électroniques du DRS qui ont causé l'atteinte à la confidentialité ou y ont contribué, lorsque le DRS désigné en vertu du paragraphe 4.4.1 juge ce nom pertinent (p. ex., collecte, utilisation ou divulgation intentionnelle des RPS par un mandataire);

- le nom de chaque DRS qui a créé et contribué à créer les renseignements personnels sur la santé du DSE;
- la date et l'heure de l'atteinte à la confidentialité;
- une description de la nature, de la portée et de la cause de l'atteinte à la confidentialité;
- une description des renseignements personnels sur la santé du DSE qui ont fait l'objet de l'atteinte à la confidentialité;
- la ou les personnes que concernent les RPS du DSE;
- les mesures prises pour confiner l'atteinte à la confidentialité;
- toute demande d'aide à cyberSanté Ontario ou aux DRS, ou aux deux, pour confiner l'atteinte à la confidentialité; et
- suffisamment d'information pour permettre d'aviser la ou les personnes que ces RPS concernent conformément à la LPRPS.

4.4.5 Le plus tôt possible, mais au plus tard à la fin du jour ouvrable suivant la réception du rapport en vertu du paragraphe 4.4.4, cyberSanté Ontario devra déclarer l'atteinte à la confidentialité à chaque DRS qui a créé ou contribué à créer les RPS et devra les aviser :

- si le DRS a seul créé ou contribué à créer les renseignements personnels sur la santé du DSE qui ont fait l'objet de l'atteinte à la confidentialité;
- le nom de chacun des dépositaires de renseignements sur la santé qui a créé et contribué à créer les RPS du DSE qui ont fait l'objet de l'atteinte à la confidentialité s'il y en a plus d'un;
- le nom de chaque DRS ou de chaque DRS dont les mandataires et les fournisseurs de services électroniques ont causé l'atteinte à la confidentialité ou y ont contribué;
- le nom de chaque mandataire et fournisseur de services électroniques du DRS qui ont causé l'atteinte à la confidentialité ou y ont contribué, lorsque le DRS désigné en vertu du paragraphe 4.4.1 juge ce nom pertinent (p. ex., collecte, utilisation ou divulgation intentionnelle des RPS par un mandataire);
- la date et l'heure de l'atteinte à la confidentialité;
- une description de la nature, de la portée et de la cause de l'atteinte à la confidentialité;
- une description des renseignements personnels sur la santé du DSE qui ont fait l'objet de l'atteinte à la confidentialité;
- la ou les personnes que concernent les RPS du DSE;
- les mesures prises pour confiner l'atteinte à la confidentialité;
- toute aide qu'on demande au DRS de fournir pour confiner l'atteinte à la confidentialité; et
- suffisamment d'information pour permettre d'aviser la ou les personnes que ces RPS concernent conformément à la LPRPS.

4.4.6 cyberSanté Ontario et les autres DRS fourniront de l'assistance dans le confinement de l'atteinte à la confidentialité lorsque le DRS désigné au paragraphe 4.4.1 la leur demande.

4.4.7 Le DRS désigné au paragraphe 4.4.1, en consultation avec les autres DRS et les autres DRS dont les mandataires et les fournisseurs de services électroniques ont causé l'atteinte à la confidentialité ou y ont contribué, déterminera également si l'atteinte à la confidentialité doit être déclarée à toute autre personne, y compris au Commissaire à l'information et à la protection de la vie privée/Ontario, aux organismes d'exécution de la loi ou de réglementation conformément à leurs politiques, leurs procédures et leurs pratiques internes.

Notification de la personne

4.4.8 Lorsque les RPS du DSE qui ont fait l'objet de l'atteinte à la confidentialité ont été créés par un autre DRS ou qu'un autre DRS y a contribué, ce dernier DRS suivra ses politiques, ses procédures et ses pratiques internes pour aviser, à la première occasion raisonnable, la ou les personnes que les DSE concernent conformément à la LPRPS et au paragraphe 4.4.11.

4.4.9 Lorsque plus d'un DRS ont créé et contribué à créer les RPS du DSE qui ont fait l'objet de l'atteinte à la confidentialité, ces DRS, le plus tôt possible, mais au plus tard 7 jours après la réception de l'information du

paragraphe 4.4.5, désigneront le DRS qui sera responsable d'aviser la ou les personnes que ces renseignements personnels sur la santé concernent conformément à la LPRPS et au paragraphe 4.4.11.

4.4.10 Pour désigner le DRS qui sera responsable d'aviser ces personnes, on tiendra compte :

- du DRS ou du DRS dont les mandataires et fournisseurs de services électroniques ont causé l'atteinte à la confidentialité ou y ont contribué;
- du DRS de qui la ou les personnes ont reçu les soins de santé les plus récents; et
- du DRS de qui la ou les personnes ont reçu le plus de soins de santé.

4.4.11 Le DRS du paragraphe 4.4.8 ou 4.4.9, selon le cas, devra aviser cette ou ces personnes et au minimum leur fournir l'information suivante :

- le nom de chaque DRS ou de chaque DRS dont les mandataires et les fournisseurs de services électroniques ont causé l'atteinte à la confidentialité ou y ont contribué;
- le nom de chaque mandataire et fournisseur de services électroniques du DRS qui ont causé l'atteinte à la confidentialité ou y ont contribué, lorsque le DRS désigné en vertu du paragraphe 4.4.1 juge ce nom pertinent (p. ex., collecte, utilisation ou divulgation intentionnelle des RPS par un mandataire);
- le nom de chaque DRS qui a créé et contribué à créer les renseignements personnels sur la santé du DSE;
- la date et l'heure de l'atteinte à la confidentialité;
- une description de la nature, de la portée et de la cause de l'atteinte à la confidentialité;
- une description des renseignements personnels sur la santé du DSE qui ont fait l'objet de l'atteinte à la confidentialité;
- les mesures prises pour confiner l'atteinte à la confidentialité;
- le nom de la personne responsable de l'enquête sur l'atteinte;
- le DRS du paragraphe 4.4.8 ou 4.4.9 selon le cas, devra, le plus tôt possible après la réception du rapport écrit approuvé par cyberSanté Ontario en vertu du paragraphe 4.4.30, fournir aux personnes le résumé des résultats de l'enquête et les mesures, connues à ce moment-là, qui ont été ou seront prises pour corriger l'atteinte à la confidentialité et pour éviter toute atteinte semblable à l'avenir;
- les mesures que la ou les personnes peuvent prendre pour protéger leurs renseignements personnels ou pour minimiser les répercussions de l'atteinte à la confidentialité, le cas échéant;
- les nom et coordonnées du DRS du paragraphe 4.4.8 ou 4.4.9, selon le cas, à qui la ou les personnes peuvent adresser leurs demandes de renseignements et leurs préoccupations; et
- l'information concernant la manière de porter plainte au Commissaire à l'information et à la protection de la vie privée/Ontario.

4.4.12 cyberSanté Ontario et les autres DRS aideront à aviser la ou les personnes que les RPS concernent lorsque le DRS leur demande de le faire en vertu du paragraphe 4.4.8 ou 4.4.9, selon le cas.

Enquête

4.4.13 cyberSanté Ontario, le ou les DRS qui ont créé et contribué à créer les RPS du dossier de santé électronique qui a fait l'objet de l'atteinte à la confidentialité ou le DRS dont les mandataires et les fournisseurs de services électroniques ont causé l'atteinte à la confidentialité ou y ont contribué devront, le plus tôt possible, mais au plus tard 7 jours après avoir déterminé qu'il y a bien eu atteinte à la confidentialité, désigner un enquêteur pour cette atteinte.

4.4.14 Pour désigner l'enquêteur pour cette atteinte en vertu du paragraphe 4.4.13, il faut :

- savoir si les DRS ou les DRS dont les mandataires et les fournisseurs de services électroniques ont causé l'atteinte à la confidentialité ou y ont contribué a la capacité de faire enquête sur l'atteinte; et
- si un autre DRS ou cyberSanté Ontario seraient mieux à même de faire enquête sur cette atteinte.

4.4.15 L'enquêteur chargé de l'atteinte à la confidentialité devra, le plus tôt possible, mais pas plus tard que 7 jours après qu'on ait déterminé qu'il y a bien eu atteinte à la confidentialité, faire enquête sur cette atteinte conformément aux politiques, aux procédures et aux pratiques internes et au paragraphe 4.4.16.

4.4.16 Dans la conduite de l'enquête, l'enquêteur devra consulter les DRS ou les DRS dont les mandataires et les fournisseurs de services électroniques ont causé l'atteinte ou y ont contribué, lorsque le DRS n'est pas l'enquêteur de cette atteinte, et devra :

- déterminer la nature, la portée et la cause de l'atteinte à la confidentialité;
- s'assurer que l'atteinte à la confidentialité a été confinée efficacement ou déterminer s'il faut prendre d'autres mesures pour la confiner;
- évaluer la pertinence des sauvegardes administratives, techniques et physiques;
- déterminer quelles mesures doivent être prises pour corriger l'atteinte à la confidentialité et pour éviter toute atteinte à la confidentialité semblable à l'avenir; et
- déterminer le calendrier et les personnes responsables de la mise en œuvre des mesures pour corriger l'atteinte à la confidentialité et pour éviter toute atteinte à la confidentialité semblable à l'avenir.

4.4.17 Les autres DRS et cyberSanté Ontario, lorsqu'ils ne sont pas responsables de l'enquête sur l'atteinte à la confidentialité, devront fournir de l'aide pour l'enquête lorsque l'enquêteur le leur demande.

4.4.18 Des rapports d'étapes pour l'enquête seront fournis par l'enquêteur lorsque cyberSanté Ontario, le ou les DRS qui ont créé ou contribué à créer les RPS du DSE qui ont fait l'objet de l'atteinte à la confidentialité ou le DRS ou le DRS dont les mandataires et les fournisseurs de services électroniques ont causé l'atteinte à la confidentialité ou y ont contribué et qu'ils ne sont pas chargés de l'enquête, le leur demande.

4.4.19 Le plus tôt possible, mais au plus tard 7 jours après l'achèvement de l'enquête, l'enquêteur de l'atteinte à la confidentialité préparera un rapport écrit qui, au minimum, contienne l'information suivante :

- le nom de chaque DRS ou de chaque DRS dont les mandataires et les fournisseurs de services électroniques ont causé l'atteinte à la confidentialité ou y ont contribué;
- le nom de chaque mandataire et fournisseur de services électroniques du DRS qui ont causé l'atteinte à la confidentialité ou y ont contribué, lorsque le DRS désigné en vertu du paragraphe 4.4.1 juge ce nom pertinent (p. ex., collecte, utilisation ou divulgation intentionnelle des RPS par un mandataire);
- le nom de chaque DRS qui a créé et contribué à créer les renseignements personnels sur la santé du DSE;
- la date et l'heure de l'atteinte à la confidentialité;
- la nature, la portée et la cause de l'atteinte à la confidentialité;
- une description des renseignements du DSE qui ont fait l'objet de l'atteinte à la confidentialité, sans divulguer aucun renseignement personnel sur la santé;
- les personnes à qui l'atteinte à la confidentialité a été déclarée en vertu du paragraphe 4.4.7;
- les mesures prises pour confiner l'atteinte à la confidentialité;
- la nature, la portée et le processus d'enquête sur l'atteinte à la confidentialité;
- les mesures qu'on recommande pour corriger l'atteinte à la confidentialité et pour éviter qu'une atteinte semblable se reproduise à l'avenir; et
- le calendrier et les personnes responsables proposées pour la mise en œuvre des mesures pour corriger l'atteinte à la confidentialité et pour éviter qu'une atteinte semblable se reproduise à l'avenir.

4.4.20 Le plus tôt possible, mais au plus tard 4 jours après l'achèvement du rapport écrit du paragraphe 4.4.19, l'enquêteur responsable de l'atteinte à la confidentialité fournira, aux fins d'examen et de commentaire, un rapport écrit à chaque DRS ou chaque DRS dont les mandataires et les fournisseurs de services électroniques ont causé l'atteinte ou y ont contribué, lorsque le DRS n'est pas chargé d'effectuer l'enquête.

4.4.21 Les DRS qui ont reçu le rapport écrit en vertu du paragraphe 4.4.20 devront, le plus tôt possible, mais au plus tard 7 jours après l'avoir reçu, l'examiner et faire des commentaires à l'enquêteur responsable de l'enquête. Si aucun commentaire n'est fourni dans les 7 jours après la réception, on tiendra pour acquis qu'il n'y a pas de commentaires.

4.4.22 Le responsable de l'enquête sur l'atteinte à la confidentialité devra, le plus tôt possible, mais au plus tard 7 jours après réception des commentaires en vertu du paragraphe 4.4.21, faire les modifications requises et fournir un rapport écrit à cyberSanté Ontario lorsque ce dernier n'est pas chargé de l'enquête.

4.4.23 Lorsque cyberSanté Ontario n'est pas chargé de l'enquête, il devra, le plus tôt possible, mais au plus tard 7 jours après l'avoir reçu en vertu du paragraphe 4.4.22, examiner le rapport écrit et faire des commentaires.

4.4.24 Le plus tôt possible, mais au plus tard 7 jours après avoir reçu ou préparé le rapport écrit du paragraphe 4.4.22, selon le cas, cyberSanté Ontario transférera le rapport écrit avec ses commentaires, le cas échéant, au DRS ou au DRS qui a créé et contribué à créer les RPS du DSE qui a fait l'objet de l'atteinte à la confidentialité aux fins d'examen et de commentaire.

4.4.25 Le ou les DRS qui ont reçu le rapport écrit en vertu du paragraphe 4.4.24 devront, le plus tôt possible, mais au plus tard 7 jours après l'avoir reçu, l'examiner et faire des commentaires à cyberSanté Ontario. Si aucun commentaire n'est fourni dans les 7 jours après la réception, on tiendra pour acquis qu'il n'y a pas de commentaires.

4.4.26 cyberSanté Ontario devra, le plus tôt possible, mais au plus tard 4 jours après avoir reçu les commentaires en vertu du paragraphe 4.4.25, aviser l'enquêteur, lorsque cyberSanté Ontario n'est pas chargé de l'enquête, de toute modification qui doit être apportée au rapport écrit ou toute mesure supplémentaire qui doit être prise pour confiner, ou rectifier l'atteinte à la confidentialité ou pour en faire l'enquête, le cas échéant.

4.4.27 Le responsable de l'enquête devra, le plus tôt possible, mais au plus tard 7 jours après avoir reçu les commentaires en vertu du paragraphe 4.4.25 ou 4.4.26, selon le cas, apporter les modifications et prendre les mesures supplémentaires requises pour confiner ou rectifier l'atteinte à la confidentialité ou pour en faire l'enquête en consultation avec les DRS ou les DRS dont les mandataires et les fournisseurs de services électroniques ont causé l'atteinte à la confidentialité ou y ont contribué, lorsque les DRS ne sont pas chargés de l'enquête, et préparer un rapport écrit révisé.

4.4.28 Lorsque cyberSanté Ontario n'est pas chargé de l'enquête, l'enquêteur qui en est chargé devra, le plus tôt possible, mais au plus tard 7 jours après avoir reçu les commentaires en vertu du paragraphe 4.4.26, fournir le rapport écrit révisé à cyberSanté Ontario.

4.4.28.1 Le plus tôt possible, mais au plus tard 4 jours après avoir reçu ou préparé le rapport écrit révisé des paragraphes 4.4.27 ou 4.4.28, selon le cas, cyberSanté Ontario transférera le rapport écrit révisé au comité de protection de la vie privée et de sécurité applicable aux fins d'examen et d'approbation et, par la suite et aux mêmes fins, à l'organisme de surveillance applicable.

4.4.28.2 Le plus tôt possible, mais au plus tard 4 jours après avoir reçu l'approbation du rapport écrit de l'organisme de surveillance applicable, cyberSanté Ontario transférera le rapport écrit approuvé à chaque DRS ou à chaque DRS dont les mandataires et les fournisseurs de services électroniques ont causé l'atteinte à la confidentialité ou y ont contribué, à chaque DRS qui a créé ou contribué à créer les RPS du DSE qui ont fait l'objet de l'atteinte et à chaque DRS responsable de la mise en œuvre des mesures pour corriger ou pour éviter toute atteinte à la confidentialité semblable à l'avenir.

4.4.29 Le DRS des paragraphes 4.4.8 ou 4.4.9, selon le cas, devra fournir à la ou aux personnes que concernent les renseignements personnels sur la santé du DSE le plus tôt possible après la réception du rapport de cyberSanté Ontario en vertu du paragraphe 4.4.30 :

- un résumé des résultats de l'enquête; et
- les mesures, connues à ce moment, qui ont été ou seront prises pour corriger l'atteinte à la confidentialité et pour éviter toute atteinte à la confidentialité semblable à l'avenir conformément à ses politiques, ses procédures et ses pratiques internes.

4.5 Procédure lorsque l'atteinte à la confidentialité a été causée uniquement par cyberSanté Ontario ou par une personne non autorisée qui n'est pas un mandataire de cyberSanté Ontario ou un DRS

Déterminer s'il y a ou non eu atteinte à la confidentialité

4.5.1 cyberSanté Ontario devra, le plus tôt possible, déterminer s'il y a eu atteinte à la confidentialité lorsqu'une atteinte à la confidentialité a été causée seulement par cyberSanté Ontario, les mandataires et les fournisseurs de services électroniques de cyberSanté Ontario ou par une personne qui n'est pas un mandataire ou un fournisseur de services électroniques de cyberSanté Ontario ou un DRS.

Confinement

4.5.2 cyberSanté Ontario lorsqu'il a déterminé qu'il y a bien eu atteinte à la confidentialité, devra suivre ses propres politiques, procédures et pratiques internes pour confiner l'atteinte à la confidentialité et, le cas échéant, demander l'aide des DRS en vertu du paragraphe 4.5.3 pour confiner l'atteinte à la confidentialité.

Déclaration aux DRS qui ont créé et contribué à créer les RPS du DSE

4.5.3 Lorsque cyberSanté Ontario a déterminé qu'il y a eu atteinte à la confidentialité ou a des motifs raisonnables de soupçonner une atteinte à la confidentialité, cyberSanté Ontario devra déclarer cette atteinte à chaque DRS qui a créé et contribué à créer les RPS du DSE le plus tôt possible, mais au plus tard à la fin du jour ouvrable suivant cette détermination. Dans sa déclaration de toute atteinte à la confidentialité, cyberSanté Ontario devra fournir toute l'information connue au moment de la déclaration, y compris :

- si cyberSanté Ontario ou ses mandataires et ses fournisseurs de services électroniques ont seuls causé l'atteinte à la confidentialité et le nom de chaque mandataire et de chaque fournisseur de services électroniques qui l'ont causé, lorsque cyberSanté Ontario juge ce nom pertinent (p. ex., consultation, manipulation ou traitement intentionnel des RPS);
- si une personne non autorisée qui n'est pas un mandataire ou un fournisseur de services électroniques de cyberSanté Ontario ou d'un DRS a seul causé l'atteinte à la confidentialité et le nom ou une description de la personne non autorisée;
- si le DRS a seul créé ou contribué à créer les renseignements personnels sur la santé du DSE qui ont fait l'objet de l'atteinte à la confidentialité;
- le nom de chacun des dépositaires de renseignements sur la santé qui a créé et contribué à créer les RPS du DSE qui ont fait l'objet de l'atteinte à la confidentialité s'il y en a plus d'un;
- la date et l'heure de l'atteinte à la confidentialité;
- une description de la nature, de la portée et de la cause de l'atteinte à la confidentialité;
- une description des renseignements personnels sur la santé du DSE qui ont fait l'objet de l'atteinte à la confidentialité;
- la ou les personnes que concernent les RPS du DSE;
- les mesures prises pour confiner l'atteinte à la confidentialité;
- toute aide qu'on demande au DRS de fournir pour confiner l'atteinte à la confidentialité; et
- suffisamment d'information pour permettre d'aviser la ou les personnes que ces RPS concernent conformément à la LPRPS.

4.5.4 Les DRS fourniront de l'assistance dans le confinement de l'atteinte à la confidentialité lorsque cyberSanté Ontario le leur demande.

4.5.5 cyberSanté Ontario avisera par écrit le Commissaire à l'information et à la protection de la vie privée/Ontario de toute atteinte à la confidentialité causée uniquement par cyberSanté Ontario ou par ses mandataires et ses fournisseurs de services électroniques.

4.5.6 cyberSanté Ontario suivra ses propres politiques, procédures et pratiques internes pour déterminer si l'atteinte à la confidentialité doit être déclarée à toute autre personne.

Notification de la personne

4.5.7 Le DRS qui a seul créé les renseignements personnels sur la santé du DSE qui ont fait l'objet de l'atteinte à la confidentialité suivra ses politiques, ses procédures et ses pratiques internes pour aviser à la première occasion raisonnable la ou les personnes que les DSE concernent conformément à la LPRPS et au paragraphe 4.5.10.

4.5.8 Lorsque plus d'un DRS ont créé ou contribué à créer les renseignements personnels sur la santé du DSE qui ont fait l'objet de l'atteinte à la confidentialité, ces DRS désigneront le plus tôt possible, mais au plus tard 7 jours après la réception de l'information du paragraphe 4.5.3, le DRS qui sera responsable d'aviser la ou les personnes que ces RPS concernent conformément à la LPRPS et au paragraphe 4.5.10.

4.5.9 Pour désigner le DRS qui sera responsable d'aviser ces personnes, on tiendra compte :

- du DRS de qui la ou les personnes ont reçu les soins de santé les plus récents; et
- du DRS de qui la ou les personnes ont reçu le plus de soins de santé.

4.5.10 Le DRS du paragraphe 4.5.7 ou 4.5.8, selon le cas, devra aviser la ou les personnes et leur fournir au minimum l'information qui suit :

- si cyberSanté Ontario ou les mandataires et les fournisseurs de services électroniques de cyberSanté Ontario ont seuls causé l'atteinte à la confidentialité et le nom de chaque mandataire et fournisseur de services électroniques qui l'ont causé, lorsque cyberSanté Ontario juge ce nom pertinent (p. ex., consultation, manipulation ou traitement non autorisés délibérés des RPS);
- si une personne non autorisée qui n'est pas un mandataire ou un fournisseur de services électroniques de cyberSanté Ontario ou d'un DRS a seul causé l'atteinte à la confidentialité et le nom ou une description de la personne non autorisée;
- le nom de chaque DRS qui a créé et contribué à créer les renseignements personnels sur la santé du DSE;
- la date et l'heure de l'atteinte à la confidentialité;
- une description de la nature, de la portée et de la cause de l'atteinte à la confidentialité;
- une description des renseignements personnels sur la santé du DSE qui ont fait l'objet de l'atteinte à la confidentialité;
- les mesures prises pour confiner l'atteinte à la confidentialité;
- le nom de la personne responsable de l'enquête sur l'atteinte;
- le DRS du paragraphe 4.5.7 ou 4.5.8 selon le cas, devra, le plus tôt possible après la réception du rapport écrit approuvé par cyberSanté Ontario en vertu du paragraphe 4.5.28, fournir aux personnes le résumé des résultats de l'enquête et les mesures, connues à ce moment-là, qui ont été ou seront prises pour corriger l'atteinte à la confidentialité et pour éviter toute atteinte semblable à l'avenir;
- les mesures que la ou les personnes peuvent prendre pour protéger leurs renseignements personnels ou pour minimiser les répercussions de l'atteinte à la confidentialité, le cas échéant;
- les nom et coordonnées du DRS du paragraphe 4.5.7 ou 4.5.8, selon le cas, à qui la ou les personnes peuvent adresser leurs demandes de renseignements et leurs préoccupations; et
- l'information concernant la manière de porter plainte au Commissaire à l'information et à la protection de la vie privée/Ontario.

4.5.11 cyberSanté Ontario et les autres DRS aideront à aviser la ou les personnes que les renseignements personnels sur la santé concernent lorsque le DRS leur demande de le faire dans le paragraphe 4.5.7 ou 4.5.8, selon le cas.

Enquête

4.5.12 cyberSanté Ontario et le ou les dépositaires de renseignements sur la santé qui ont créé ou contribué à créer les RPS du DSE qui ont fait l'objet de l'atteinte à la confidentialité devront, le plus tôt possible, mais au plus tard 7 jours après avoir déterminé qu'il y a bien eu atteinte à la confidentialité, désigner un enquêteur pour cette atteinte.

4.5.13 Pour désigner l'enquêteur pour cette atteinte en vertu du paragraphe 4.5.12, il faut juger :

- si cyberSanté Ontario a la capacité de faire enquête sur cette atteinte à la confidentialité et;
- si un DRS serait mieux à même de faire enquête sur cette atteinte.

4.5.14 L'enquêteur chargé de l'atteinte à la confidentialité devra, le plus tôt possible, mais pas plus tard que 7 jours après qu'on ait déterminé qu'il y a bien eu atteinte à la confidentialité, faire enquête sur cette atteinte conformément aux politiques, aux procédures et aux pratiques internes et au paragraphe 4.5.15.

4.5.15 Dans la conduite de cette enquête, l'enquêteur devra consulter cyberSanté Ontario lorsque cyberSanté Ontario n'est pas chargé de cette enquête, et devra :

- déterminer la nature, la portée et la cause de l'atteinte à la confidentialité;
- s'assurer que l'atteinte à la confidentialité a été confinée efficacement ou déterminer s'il faut prendre d'autres mesures pour la confiner;
- évaluer la pertinence des sauvegardes administratives, techniques et physiques;
- déterminer quelles mesures doivent être prises pour corriger l'atteinte à la confidentialité et pour éviter toute atteinte à la confidentialité semblable à l'avenir; et
- déterminer le calendrier et les personnes responsables de la mise en œuvre des mesures pour corriger l'atteinte à la confidentialité et pour éviter toute atteinte à la confidentialité semblable à l'avenir.

4.5.16 Les autres DRS et cyberSanté Ontario, lorsqu'ils ne sont pas chargés de l'enquête sur l'atteinte à la confidentialité, devront participer à l'enquête lorsque l'enquêteur le leur demande.

4.5.17 L'enquêteur fournira des rapports d'enquête lorsque cyberSanté Ontario ou le ou les DRS qui ont créé ou contribué à créer les renseignements personnels sur la santé du dossier de santé électronique qui ont fait l'objet de l'atteinte à la confidentialité lorsqu'ils ne sont pas chargés de l'enquête, le leur demande.

4.5.18 Le plus tôt possible, mais au plus tard 7 jours après l'achèvement de l'enquête, l'enquêteur de l'atteinte à la confidentialité préparera un rapport écrit qui, au minimum, contienne l'information suivante :

- si cyberSanté Ontario ou ses mandataires ou ses fournisseurs de services électroniques ont seuls causés l'atteinte à la confidentialité;
- le nom de chaque mandataire ou de chaque fournisseur de services électroniques de cyberSanté Ontario qui ont causé l'atteinte à la confidentialité, le cas échéant, lorsque cyberSanté Ontario juge ce nom pertinent (p. ex., consultation, manipulation ou traitement non autorisés délibérés);
- si une personne non autorisée qui n'est pas un mandataire ou un fournisseur de services électroniques de cyberSanté Ontario ou un DRS ont seul causé l'atteinte à la confidentialité;
- le nom ou une description de la personne non autorisée, le cas échéant;
- le nom de chaque DRS qui a créé et contribué à créer les renseignements personnels sur la santé du DSE;
- la date et l'heure de l'atteinte à la confidentialité;
- la nature, la portée et la cause de l'atteinte à la confidentialité;
- une description des renseignements du DSE qui ont fait l'objet de l'atteinte à la confidentialité, sans divulguer aucun renseignement personnel sur la santé;
- les personnes à qui l'atteinte à la confidentialité a été déclarée en vertu des paragraphes 4.5.5 et 4.5.6;
- les mesures prises pour confiner l'atteinte à la confidentialité;
- la nature, la portée et le processus d'enquête sur l'atteinte à la confidentialité;
- les mesures qu'on recommande pour corriger l'atteinte à la confidentialité et pour éviter qu'une atteinte semblable se reproduise à l'avenir; et
- le calendrier et les personnes responsables proposées pour la mise en œuvre des mesures pour corriger l'atteinte à la confidentialité et pour éviter qu'une atteinte semblable se reproduise à l'avenir.

4.5.19 Le plus tôt possible, mais au plus tard 4 jours après l'achèvement du rapport écrit du paragraphe 4.5.18, l'enquêteur chargé de l'atteinte à la confidentialité fournira, aux fins d'examen et de commentaire, un rapport écrit à cyberSanté Ontario lorsque cyberSanté Ontario n'est pas chargé d'effectuer l'enquête.

4.5.20 Lorsque cyberSanté Ontario n'est pas chargé de l'enquête, il devra, le plus tôt possible, mais au plus tard 7 jours après avoir reçu le rapport écrit en vertu du paragraphe 4.5.19, l'examiner et faire des commentaires

à l'enquêteur. Si aucun commentaire n'est fourni dans les 7 jours après la réception, on tiendra pour acquis qu'il n'y a pas de commentaires.

4.5.21 Lorsque cyberSanté Ontario n'est pas chargé de l'enquête sur l'atteinte à la confidentialité, l'enquêteur qui en est chargé devra, le plus tôt possible, mais au plus tard 7 jours après avoir reçu les commentaires en vertu du paragraphe 4.5.20, apporter les modifications requises et fournir le rapport écrit à cyberSanté Ontario.

4.5.22 Le plus tôt possible, mais au plus tard 7 jours après avoir reçu ou préparé le rapport écrit des paragraphes 4.5.18 ou 4.5.21, selon le cas, cyberSanté Ontario le transférera, aux fins d'examen et de commentaire, aux DRS qui ont créé et contribué à créer les renseignements personnels sur la santé du DSE qui ont fait l'objet de l'atteinte à la confidentialité.

4.5.23 Le ou les DRS qui ont reçu le rapport écrit en vertu du paragraphe 4.5.22 devront, le plus tôt possible, mais au plus tard 7 jours après l'avoir reçu, l'examiner et faire des commentaires à cyberSanté Ontario. Si aucun commentaire n'est fourni dans les 7 jours après la réception, on tiendra pour acquis qu'il n'y a pas de commentaires.

4.5.24 cyberSanté Ontario devra, le plus tôt possible, mais au plus tard 4 jours après avoir reçu les commentaires en vertu du paragraphe 4.5.23, aviser l'enquêteur, lorsque cyberSanté Ontario n'est pas chargé de l'enquête, de toute modification qui doit être apportée au rapport écrit ou toute mesure supplémentaire qui doit être prise pour confiner, ou rectifier l'atteinte à la confidentialité ou pour en faire l'enquête, le cas échéant.

4.5.25 Le responsable de l'enquête devra, le plus tôt possible, mais au plus tard 7 jours après avoir reçu les commentaires en vertu des paragraphes 4.5.23 ou 4.5.24, selon le cas, apporter les modifications et prendre les mesures supplémentaires pour confiner ou rectifier l'atteinte à la confidentialité ou en faire l'enquête en consultation avec cyberSanté Ontario, lorsque cyberSanté Ontario n'est pas chargé de l'enquête, et préparer un rapport écrit révisé.

4.5.26 Lorsque cyberSanté Ontario n'est pas chargé de l'enquête, l'enquêteur qui en est chargé devra, le plus tôt possible, mais au plus tard 7 jours après avoir reçu les commentaires en vertu du paragraphe 4.5.24, fournir le rapport écrit révisé à cyberSanté Ontario.

4.5.26.1 Le plus tôt possible, mais au plus tard 4 jours après avoir reçu ou préparé le rapport écrit révisé des paragraphes 4.5.25 ou 4.5.26, selon le cas, cyberSanté Ontario transférera le rapport écrit révisé au comité de protection de la vie privée et de sécurité applicable aux fins d'examen et d'approbation et, par la suite et aux mêmes fins, à l'organisme de surveillance applicable.

4.5.27 Le plus tôt possible, mais au plus tard 4 jours après avoir reçu l'approbation du rapport écrit de l'organisme de surveillance applicable, cyberSanté Ontario transférera le rapport écrit approuvé à chaque dépositaire de renseignements sur la santé qui a créé ou contribué à créer les RPS du DSE qui ont fait l'objet de l'atteinte et à chaque DRS responsable de la mise en œuvre des mesures pour rectifier ou pour éviter toute atteinte à la confidentialité semblable à l'avenir.

4.5.28 Le DRS des paragraphes 4.5.7 ou 4.5.8, selon le cas, devra le plus tôt possible après réception du rapport de cyberSanté Ontario en vertu du paragraphe 4.5.28, fournir à la ou aux personnes que concernent les renseignements personnels sur la santé du DSE :

- un résumé des résultats de l'enquête; et
- les mesures, connues à ce moment, qui ont été ou seront prises pour corriger l'atteinte à la confidentialité et pour éviter toute atteinte à la confidentialité semblable à l'avenir conformément à ses politiques, ses procédures et ses pratiques internes.

4.6 Procédure relative à la rectification des atteintes à la confidentialité

4.6.1.1 cyberSanté Ontario et les DRS mettront en œuvre les mesures énumérées dans le rapport écrit approuvé par l'organisme de surveillance applicab****le pour rectifier et pour éviter toute atteinte semblable à l'avenir.

4.6.2 Chaque DRS responsable de la mise en œuvre des mesures correctrices ou d'éviter toute atteinte semblable à l'avenir devra, tous les 30 jours, jusqu'à ce que les mesures dont le DRS est responsable aient été mises en œuvre, fournir un rapport écrit à cyberSanté Ontario qui établit :

- les mesures dont la mise en œuvre incombe au DRS et le calendrier de mise en œuvre de chaque mesure énumérée dans le rapport écrit approuvé par l'organisme de surveillance applicable;
- l'état et la date ou la date cible de mise en œuvre de chaque mesure; et

- la manière, prévue ou réelle, de mettre en œuvre chaque mesure.

4.6.3 Chaque mandataire ou fournisseur de services électroniques du DRS ou de cyberSanté Ontario qui a causé l'atteinte à la confidentialité en collectant, utilisant ou divulguant, ou en consultant, manipulant ou traitant autrement les RPS d'une manière non autorisée, pourrait faire l'objet d'une vérification supplémentaire conformément à la *Politique sur la journalisation et la surveillance du dossier de santé électronique* et ses procédures connexes, telles que modifiées de temps à autre.

4.7 Procédure relative à la tenue d'un journal des atteintes à la confidentialité

4.7.1 cyberSanté Ontario tiendra un journal des atteintes à la confidentialité qui contiendra pour chacune d'elles :

- le cas échéant, le nom de chaque DRS ou de chaque DRS dont les mandataires ou les fournisseurs de services électroniques ont causé l'atteinte à la confidentialité ou y ont contribué et le nom de chaque mandataire et fournisseur de services électroniques du DRS qui a causé l'atteinte à la confidentialité ou y a contribué, lorsque ce nom a été jugé pertinent conformément à la politique et à ses procédures connexes;
- le cas échéant, que cyberSanté Ontario ou ses mandataires ou ses fournisseurs de services électroniques ont seuls causé l'atteinte à la confidentialité et le nom de chaque mandataire et fournisseur de services électroniques de cyberSanté Ontario qui a causé l'atteinte à la confidentialité, lorsque ce nom a été jugé pertinent conformément à la politique et à ses procédures connexes;
- le cas échéant, qu'une personne non autorisée qui n'est pas un mandataire ou un fournisseur de services électroniques de cyberSanté Ontario ou d'un DRS a seul causé l'atteinte à la confidentialité et le nom ou une description de la personne non autorisée;
- le nom de chaque DRS qui a créé et contribué à créer les renseignements personnels sur la santé du DSE;
- la date et l'heure de l'atteinte à la confidentialité;
- la nature, la portée et la cause de l'atteinte à la confidentialité;
- une description des renseignements du DSE qui ont fait l'objet de l'atteinte à la confidentialité, sans divulguer aucun renseignement personnel sur la santé;
- les mesures prises pour confiner l'atteinte à la confidentialité;
- les mesures prises ou qui seront prises pour rectifier l'atteinte à la confidentialité et pour éviter qu'une atteinte semblable se reproduise à l'avenir;
- le calendrier et les personnes responsables de la mise en œuvre des mesures pour rectifier l'atteinte à la confidentialité et pour éviter qu'une atteinte semblable se reproduise à l'avenir;
- l'état, la date ou la date cible de la mise en œuvre des mesures prises pour corriger l'atteinte à la confidentialité et pour éviter que toute atteinte semblable se reproduise à l'avenir; et
- la manière, prévue ou réelle, de mettre en œuvre chaque mesure.

4.7.2 cyberSanté Ontario vérifiera et surveillera le journal du paragraphe 4.7.1 pour :

- repérer les constantes et les tendances des atteintes à la confidentialité;
- cerner les sauvegardes administratives, techniques et physiques qui doivent être mises en œuvre pour éviter les atteintes à la confidentialité ou en réduire le risque; et
- s'assurer que des mesures sont prises pour corriger l'atteinte à la confidentialité et pour éviter qu'une atteinte semblable se reproduise à l'avenir.

4.7.3 cyberSanté Ontario transférera, tous les 30 jours, un rapport écrit sur l'état de la mise en œuvre des mesures prises pour rectifier l'atteinte à la confidentialité et pour éviter qu'une atteinte semblable se reproduise à l'avenir à chaque DRS et à chaque DRS dont les mandataires et fournisseurs de services électroniques ont causé l'atteinte à la confidentialité ou y ont contribué, à chaque DRS qui a créé ou contribué à créer les RPS du DSE qui ont fait l'objet de l'atteinte et à chaque DRS responsable de la mise en œuvre des mesures pour corriger ou prévenir toute atteinte à la confidentialité semblable à l'avenir.

4.7.4 cyberSanté Ontario fournira un rapport écrit sur l'état de la mise en œuvre des mesures prises pour corriger l'atteinte à la confidentialité et pour éviter qu'une atteinte semblable se reproduise à l'avenir à

chaque réunion du comité de protection de la vie privée et de sécurité applicable et à l'organisme de surveillance applicable, ou plus souvent si le comité de protection de la vie privée et de sécurité applicable et l'organisme de surveillance applicable le demandent.

4.7.5 Au minimum, le rapport écrit des paragraphes 4.7.3 et 4.7.4 doit établir :

- les mesures dont la mise en œuvre incombe à cyberSanté Ontario et aux DRS et le calendrier de mise en œuvre de chaque mesure énumérée dans le rapport écrit approuvé par l'organisme de surveillance applicable;
- l'état et la date ou la date cible de mise en œuvre de chaque mesure; et
- la manière, prévue ou réelle, de mettre en œuvre chaque mesure.

5 Exécution[3]

5.1.1 Le DRS examinera tous les cas de non-conformité de ses mandataires ou de ses fournisseurs de services électroniques et cyberSanté Ontario examinera tous les cas de non-conformité de ses mandataires ou de ses fournisseurs de services électroniques. Le DRS ou cyberSanté Ontario, selon le cas, imposera les sanctions appropriées à tout mandataire ou fournisseur de services électroniques et exigera la mise en œuvre de mesures correctrices conformément à ses politiques, ses procédures et ses pratiques internes.

5.1.2 Le comité de protection de la vie privée et de sécurité applicable examinera tous les cas de non-conformité. Le comité de protection de la vie privée et de sécurité applicable recommandera les mesures appropriées à l'organisme de surveillance applicable.

5.1.3 L'organisme de surveillance pertinent a le pouvoir d'imposer les sanctions appropriées, jusqu'à et y compris la fin de l'accord en la matière avec le DRS ou la fin des privilèges d'accès des mandataires et des fournisseurs de services électroniques, et d'exiger la mise en œuvre de mesures correctrices.

6 Glossaire

Dossier de santé électronique (DSE)
Ensemble de la solution ConnexionOntario et du Dépôt des Services communs d'imagerie diagnostique, soit des dépôts ou des systèmes auxiliaires cliniques destinés à stocker et à rendre accessibles des renseignements personnels sur la santé contenus dans les systèmes électroniques de renseignements sur la santé des dépositaires de ces renseignements de manière à ne créer qu'un seul dépôt.

Enquêteur
Tout DRS ou tout employé de cyberSanté Ontario qui est choisi pour diriger une enquête sur une atteinte à la confidentialité par cyberSanté Ontario, le ou les DRS qui ont créé ou contribué à créer les RPS du DSE qui ont fait l'objet de cette atteinte à la confidentialité et le ou les DRS qui ont causé ou dont les mandataires et fournisseurs de services électroniques ont causé l'atteinte à la confidentialité, selon le cas.

Accords en la matière
Les accords relatifs au DSE signés par le DRS, cyberSanté Ontario, les mandataires et les fournisseurs de services électroniques d'un DRS, ou les mandataires et les fournisseurs de services électroniques de cyberSanté Ontario.

Fournisseur de services électroniques
Personne qui fournit des biens ou des services dans le but de permettre à un dépositaire de renseignements sur la santé d'employer des moyens électroniques de recueillir, d'utiliser, de modifier, de divulguer, de conserver ou d'éliminer des renseignements personnels sur la santé et qui comprend un fournisseur de réseau d'information sur la santé.

[3] *Le Tableau 1 : Organismes de gestion appropriés* renvoie au comité de protection de la vie privée et de sécurité applicable et à l'organisme de surveillance applicable.

Atteinte à la confidentialité
Une atteinte à la confidentialité comprend les circonstances dans lesquelles :

- une disposition de la LPRPS ou son règlement a été enfreinte;
- les dispositions sur la protection des renseignements personnels des accords applicables relatives au DSE ont été enfreintes;
- les politiques, les procédures et les pratiques en matière de protection des renseignements personnels relatives au DSE ont été enfreintes;
- les RPS du DSE sont perdus ou volés ou ont été consultés par une personne non autorisée; et
- les RPS du DSE ont été copiés, modifiés ou éliminés de manière non autorisée.

Structure d'administration de la politique	Solution ConnexionOntario	Dépôt des Services communs d'imagerie diagnostique
Comité de protection de la vie privée et de sécurité applicable	Protection de la vie privée : Comité de protection de la vie privée (Connecting Privacy) Sécurité : Comité de sécurité (Connecting Security)	Protection de la vie privée : Groupe de travail sur la protection de la vie privée et la sécurité des Services communs d'imagerie diagnostique Sécurité : Comité de sécurité (Connecting Security)
Organisme de surveillance applicable	Protection de la vie privée : Comité directeur de ConnexionOntario Sécurité : Comité stratégique de cyberSanté Ontario	Protection de la vie privée : Comité exécutif des Services communs d'imagerie diagnostique Sécurité : Comité stratégique de cyberSanté Ontario

Tableau 1: Organisme de gouvernance applicable

Terme ou acronyme	Définition
DRS	Dépositaire de renseignements sur la santé
RPS	Renseignements personnels sur la santé, tel que le terme est défini dans la *Loi de 2004 sur la protection des renseignements personnels sur la santé*
LPRPS	*Loi de 2004 sur la protection des renseignements personnels sur la santé*

7 Références et documents connexes

Loi de 2004 sur la protection des renseignements personnels sur la santé (LPRPS)
Commissaire à l'information et à la protection de la vie privée/Ontario : Ce qu'il faut faire en cas d'atteinte à la confidentialité : Lignes directrices pour le secteur de la santé
Politique sur les demandes de renseignements et les plaintes relatives au dossier de santé électronique et ses procédures connexes
Politique sur la journalisation et la surveillance du dossier de santé électronique et ses procédures connexes
Politique sur la formation en protection des renseignements personnels et en sécurité du dossier de santé électronique et ses procédures connexes

eHealth Ontario

Politique de conservation

Dossier de santé électronique

Version : 2.0

N° de document : 4033

Ontario
eHealth Ontario

Gestion du document

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

Historique des approbations

APPROBATEURS	DATE D'APPROBATION
Membres du comité de protection de la vie privée ConnectingPrivacy	8 décembre 2016

Historique des révisions

VERSION Nº	DATE AAA-MM-JJ	RÉSUMÉ DES CHANGEMENTS	AUTEUR
2.0	2016-12-01	Révisions conformément à l'évaluation des politiques par le CPC	Rand Muhtam, analyste en protection de la vie privée, cyberSanté Ontario
1.1	2015-11-25	Révisions mineures – mise à jour pour ConnexionOntario	Samara Strub, analyste en protection de la vie privée, cyberSanté Ontario
1.0	2015-06-10	Version définitive	Promila Gonsalves, Analyste principale des systèmes de gestion de la vie privée, cyberSanté Ontario
0.01	2015-03-05	Version initiale fondée sur la version 1.0 de la politique de conservation harmonisée du comité ConnectingPrivacy	Promila Gonsalves, Analyste principale des systèmes de gestion de la vie privée, cyberSanté Ontario

Table des matières

1 Objectif

Définir les politiques et les procédures régissant la conservation des dossiers dans le cadre de l'utilisation du dossier de santé électronique (DSE).

2 Portée

La présente politique et les procédures connexes s'appliquent à la conservation des dossiers suivants dans le cadre de l'utilisation du DSE :

- Les renseignements personnels sur la santé (RPS);
- Les renseignements personnels recueillis pour appuyer le Registre de fournisseurs (RP);
- Les journaux et rapports de vérification renfermant des RPS ou des RP;
- Les renseignements recueillis au sujet d'un particulier afin de répondre :
    - aux demandes d'accès ou aux demandes de rectification en vertu de la *Loi de 2004 sur la protection des renseignements personnels sur la santé* (LPRPS);
    - aux demandes visant à donner, à modifier ou à retirer une directive en matière de consentement en vertu de la LPRPS;
    - aux demandes de renseignements ou aux plaintes déposées en vertu de la LPRPS;
- Les renseignements créés au sujet d'un particulier dans le cadre d'une enquête sur des violations touchant la protection de la vie privée et(ou) des incidents de sécurité;
- Les journaux système, les journaux de suivi, les rapports et les documents connexes servant à l'exécution de tâches liées à la protection de la vie privée et à la sécurité, et ne renfermant pas de RPS ou de RP;
- Les documents institutionnels rassemblés ou créés par cyberSanté Ontario, notamment :
    - les modèles ou les ressources élaborés par cyberSanté dans le cadre de l'utilisation du DSE;
    - les documents liés aux assurances;
    - les documents opérationnels de cyberSanté Ontario.

La présente politique et les procédures connexes ne s'appliquent pas aux copies des dossiers de RPS ou de RP qui ont été faites à partir du DSE et conservées par le dépositaire de renseignements sur la santé (DRS), ou par les mandataires ou les fournisseurs de services électroniques du DRS, autres que cyberSanté Ontario et ses mandataires ou fournisseurs de services électroniques.

Le DSE renferme des données provenant de la solution ConnexionOntario et du Dépôt du Service commun d'imagerie diagnostique, les deux étant considérés comme des dépôts de données cliniques et(ou) des systèmes auxiliaires, conçus pour stocker et rendre accessibles certains renseignements électroniques personnels sur la santé tirés des systèmes électroniques d'information sur la santé des DRS[1].

[1] Les divergences entre les exigences des politiques et des procédures de la solution ConnexionOntario et du Dépôt du Service commun d'imagerie diagnostique sont indiquées dans la présente politique.

3 Politique

3.1 Politiques et principes directeurs

3.1.1 La LPRPS exige du DRS qu'il s'assure que les dossiers de RPS ou de RP dont il a la garde ou le contrôle soient conservés, transférés et éliminés de manière sécuritaire conformément aux exigences prescrites dans la LPRPS.

3.1.2 La LPRPS exige du DRS qu'il conserve les dossiers de RPS ayant fait l'objet d'une demande d'accès prévue à l'article 53 aussi longtemps que nécessaire pour permettre au particulier d'épuiser tout recours prévu par la LPRPS qu'il peut avoir à l'égard de la demande.

3.1.3 Les DRS et cyberSanté Ontario adoptent et tiennent à jour les politiques, les procédures et les pratiques en matière de protection de la vie privée et de sécurité nécessaires pour s'acquitter de leurs obligations en vertu de la LPRPS, de la *Loi de 1990 sur l'accès à l'information et la protection de la vie privée* (LAIPVP) ou, le cas échéant, de la *Loi de 1990 sur l'accès à l'information municipale et la protection de la vie privée* (LAIMPVP), des ententes applicables, ainsi que de la présente politique et de ses procédures connexes.

3.1.4 Les DRS et cyberSanté Ontario adoptent et tiennent à jour des politiques, des procédures et des pratiques en matière de protection de la vie privée et de sécurité qui sont conformes à la LPRPS et à la LAIPVP/LAIMPVP, le cas échéant, et informent leurs mandataires et fournisseurs de services électroniques de la teneur de ces politiques, procédures et pratiques comme l'exigent la LPRPS et la LAIPVP/LAIMPVP, le cas échéant.

3.1.5 cyberSanté Ontario se dote d'un programme qui lui permet, tout comme à ses DRS, de s'acquitter de ses obligations en ce qui a trait à la conservation des dossiers de RPS ou de RP en conformité avec la LPRPS, la LAIPVP/LAIMPVP, le cas échéant, les ententes applicables, ainsi que la présente politique et ses procédures connexes.

3.1.6 Les DRS et cyberSanté Ontario prennent des mesures raisonnables dans les circonstances pour s'assurer que leurs mandataires et fournisseurs de services électroniques respectent la LPRPS, la LAIPVP/LAIMPVP, le cas échéant, les ententes applicables, ainsi que la présente politique et ses procédures connexes.

3.1.7 Dans le cadre de l'utilisation du DSE, les DRS et cyberSanté Ontario tiennent à jour des dossiers en conformité avec les lois applicables, les règlements professionnels, les pratiques généralement reconnues dans l'industrie, la présente politique et ses procédures connexes, ainsi que leurs politiques, procédures et pratiques internes.

4 Procédures

4.1 Procédures liées à la conservation des dossiers

4.1.1 cyberSanté Ontario et les DRS veillent à ce que les dossiers mentionnés à la section 4.3 soient conservés pendant le délai indiqué à la section 4.3. Diverses méthodes de stockage peuvent être utilisées, à condition que les dossiers soient conservés de manière sécuritaire et puissent être récupérés dans le laps de temps requis.

4.1.2 cyberSanté Ontario et les DRS veillent à ce que les renseignements non mentionnés à la section 4.3 soient conservés aussi longtemps que nécessaire dans le cadre de l'utilisation du DSE.

4.1.3 Les DRS et cyberSanté Ontario, de même que leurs mandataires et fournisseurs de services électroniques, prennent des mesures raisonnables dans les circonstances pour veiller à ce que les dossiers soient protégés contre le vol, la perte et une utilisation ou une divulgation non autorisée, de même que contre une duplication, une modification ou une élimination non autorisée, qu'ils soient inactifs ou de passage, en adhérant à la *Politique de sécurité de l'information* dans le contexte du DSE et à la politique sur la gestion des actifs et de l'information (*Information and Asset Management Policy*) et à ses politiques et procédures connexes, et à leurs versions modifiées lorsqu'il y a lieu.

Procédures supplémentaires relatives à la conservation des RPS et des RP

4.1.4 cyberSanté Ontario veille à ce que le DSE soit en mesure de conserver les dossiers de RPS ou de RP aussi longtemps que nécessaire, conformément à la section 4.3.

4.1.5 À la fin du calendrier de conservation indiqué à la section 4.3, le DSE ne mettra plus les RPS ou les RP à la disposition des DRS ou de cyberSanté Ontario, ou à celle de leurs mandataires ou fournisseurs de services électroniques.

4.1.6 Malgré le paragraphe 4.1.4, lorsque prendra fin la relation entre cyberSanté Ontario et le DRS qui a créé et saisi les RPS ou les RP dans le DSE, le comité de protection de la vie privée et de sécurité applicable collaborera avec ce DRS pour qu'il dispose des RPS en conformité avec la LPRPS, les ententes applicables, la présente politiques et ses politiques et procédures connexes, et avec leurs versions modifiées lorsqu'il y a lieu.

4.1.7 Lorsque les RPS ou les RP figurant dans le DSE décrits au paragraphe 4.1.6 ont été recueillis par un DRS autre que celui qui les a créés et saisis, ils seront conservés dans le DSE pendant le délai indiqué à la section 4.3 et pourront être

recueillis, utilisés et divulgués ultérieurement par les DRS et cyberSanté Ontario, ainsi que leurs mandataires et fournisseurs de services électroniques.

4.1.8 Lorsque les RPS ou les RP figurant dans le DSE décrits au paragraphe 4.1.6 n'ont pas été recueillis par un DRS autre que celui qui les a créés et saisis, ils seront conservés dans le DSE pendant le délai indiqué à la section 4.3, mais ne seront plus accessibles et ne pourront pas être recueillis, utilisés et divulgués ultérieurement par les DRS et cyberSanté Ontario, ainsi que leurs mandataires et fournisseurs de services électroniques.

4.2 Procédures liées à l'élimination des dossiers en toute sécurité

4.2.1 Les DRS et cyberSanté Ontario, ainsi que leurs mandataires et fournisseurs de services électroniques, veillent à ce que les dossiers soient éliminés de manière sécuritaire, de sorte que leur reconstitution ne soit pas raisonnablement prévisible dans les circonstances, et en conformité avec les politiques et procédures établies dans la *Politique de sécurité de l'information* et ses politiques et procédures associées, et avec leurs versions modifiées lorsqu'il y a lieu.

4.3 Calendrier de conservation

cyberSanté Ontario et les DRS, le cas échéant, conservent les dossiers renfermant les renseignements décrits dans le tableau ci-dessous pendant le délai indiqué :

Type de renseignements[2]	**Délai de conservation**
RPS figurant dans le DSE	Le plus long des délais indiqués ci-dessous : • Pendant aussi longtemps que le DRS qui a créé et saisi les RPS dans le DSE conserve ces derniers dans ses systèmes locaux; • Pendant les délais indiqués dans le calendrier de conservation établi par le DRS qui a créé et saisi les RPS dans le DSE; • Trente ans après le dernier cas de consultation, d'emploi ou de traitement d'une autre manière des RPS dans le but de fournir des soins de santé ou d'aider à leur prestation; ou 10 ans après le décès du patient et en conformité avec toute ordonnance ou décision judiciaire applicable, ou toute autre exigence prévue par la loi
Journaux et rapports de vérification renfermant des RPS : • Créés et maintenus à des fins de conformité • Créés et maintenus à des fins de dépannage	Trente ans ou lorsque les RPS sont supprimés du DSE, selon le délai le plus long Conserver les journaux d'audit et les rapports d'audit qui contiennent des RPS créés et maintenus à des fins de dépannage et d'autres fins opérationnelles tant qu'ils sont nécessaires, mais pas plus de 60 jours, sauf si la directrice de la protection de la vie privée de cyberSanté Ontario ou son remplaçant permet qu'ils soient conservés plus longtemps.
Copies archivées : o des RPS figurant dans le DSE; o des journaux et rapports de vérification renfermant des RPS	Équivalent du délai de conservation des RPS figurant dans le DSE ou les journaux et rapports de vérification, respectivement
Copies de sauvegarde : o des RPS figurant dans le DSE; o des journaux et rapports de vérification renfermant des RPS	Destruction des données en toute sécurité selon le calendrier établi par le fournisseur de services électroniques, mais conservation pendant une durée maximale de 2 ans

[2] L'Annexe A renferme de plus amples détails sur les types de renseignements.

Type de renseignements[2]	Délai de conservation
Renseignements recueillis pour répondre aux demandes de particuliers concernant : o leur demande d'accès ou leur demande de rectification en vertu de la LPRPS; o leur demande visant à donner, à modifier ou à retirer une directive en matière de consentement en vertu de la LPRPS; o leur demande de renseignements ou leur plainte déposée en vertu de la LPRPS	Deux ans après la fermeture du dossier de demande d'accès, de demande de rectification, de demande visant à donner, à modifier ou à retirer une directive en matière de consentement, ou de demande de renseignements Dans le cas des plaintes, deux après la fermeture, par le DRS, cyberSanté Ontario ou le Commissaire à l'information et à la protection de la vie privée de l'Ontario, du dossier de plainte, selon le délai le plus long
Renseignements créés au sujet d'un particulier dans le cadre d'une enquête sur des violations touchant la protection de la vie privée et(ou) des incidents de sécurité	Deux ans après la fermeture, par le DRS, cyberSanté Ontario ou le Commissaire à l'information et à la protection de la vie privée de l'Ontario, du dossier de violation touchant la protection de la vie privée, selon le délai le plus long
Renseignements utilisés aux fins d'identification ou d'insription du fournisseur et qui contiennent des	Sept ans après la dernière utilisation
Authentifiants d'un utilisateur final pour lequel un DRS est un fournisseur d'identité	De façon permanente
Journaux système, journaux de suivi, rapports et documents connexes servant à l'exécution de tâches liées à la protection de la vie privée et à la sécurité, et ne renfermant pas de RPS	Délai minimal de deux ans
Événements d'authentification pour lesquels un DRS est un fournisseur d'identité	60 jours en ligne, total de 24 mois dans des archives
Modèles ou ressources élaborés par cyberSanté dans le cadre de l'utilisation du DSE	Délai minimal de deux ans
Documents liés aux assurances	Dix ans
Documents opérationnels de cyberSanté Ontario	Délai minimal de sept ans

5 Application[3]

5.1.1 Tous les cas de non-respect seront examinés par le comité de protection de la vie privée et de sécurité applicable. Le comité de protection de la vie privée et de sécurité applicable recommandera la voie à suivre à l'organisme de surveillance applicable.

5.1.2 L'organisme de surveillance applicable a le pouvoir d'imposer les sanctions appropriées, ce qui peut inclure la cessation des ententes applicables avec le DRS ou la cessation des privilèges d'accès des mandataires et des fournisseurs de services électroniques et une demande de mesures correctives.

6 Glossaire

Dossier de santé électronique (DSE)
Ensemble de la solution ConnexionOntario et du Dépôt du Service commun d'imagerie diagnostique, soit des dépôts ou des systèmes auxiliaires cliniques destinés à stocker et à rendre accessibles des RPS contenus dans les systèmes électroniques de renseignements sur la santé des dépositaires de ces renseignements de manière à ne créer qu'un seul référentiel.

Plainte
Le terme « plainte » a le même sens que celui prévu dans la politique sur la gestion des demandes de renseignements et des plaintes dans le cadre de l'utilisation du DSE (*Electronic Health Record Inquiries and Complaints Policy*) et ses procédures connexes, et dans leurs versions modifiées lorsqu'il y a lieu.

[3] Les références au comité de protection de la vie privée et de sécurité applicable et à l'organisme de surveillance applicable se trouvent au *Tableau 1 : Organismes administratifs applicables*.

Directive en matière de consentement
L'expression « directive en matière de consentement » a le même sens que celui prévu dans la politique sur la gestion du consentement dans le cadre de l'utilisation du DSE (*Electronic Health Record Consent Management Policy*) et ses procédures connexes, et dans leurs versions modifiées lorsqu'il y a lieu.

Fournisseur de services électroniques
Personne qui fournit des biens ou des services dans le but de permettre à un dépositaire de renseignements sur la santé d'employer des moyens électroniques de recueillir, d'utiliser, de modifier, de diffuser, de conserver ou d'éliminer des RPS et qui comprend un fournisseur de réseau d'information sur la santé.

Demande de renseignements
L'expression « demande de renseignements » a le même sens que celui prévu dans la *Politique relative aux plaintes et aux demandes de renseignements liées à la protection de la vie privée concernant les dossiers de santé électroniques* et ses procédures connexes, et dans leurs versions modifiées lorsqu'il y a lieu.

Violation touchant la protection de la vie privée
L'expression « violation touchant la protection de la vie privée » a le même sens que celui prévu dans la *Politique de gestion des atteintes à la confidentialité relatives aux dossiers de santé électroniques* et ses procédures connexes, et dans leurs versions modifiées lorsqu'il y a lieu.

Demande d'accès
L'expression « demande d'accès » a le même sens que celui prévu dans la *Politique sur l'accès aux renseignements et la rectification des renseignements concernant les dossiers de santé électroniques* et ses procédures connexes, et dans leurs versions modifiées lorsqu'il y a lieu.

Demande de rectification
L'expression « demande de rectification » a le même sens que celui prévu dans la P*olitique sur l'accès aux renseignements et la rectification des renseignements concernant les dossiers de santé électroniques et* ses procédures connexes, et dans leurs versions modifiées lorsqu'il y a lieu .

Structure d'administration de la politique	Solution ConnexionRGT	Dépôt d'imagerie diagnostique des services hospitaliers
Comité de protection de la vie privée et de sécurité applicable	Protection de la vie privée : Comité de protection de la vie privée (Connecting Privacy) Sécurité : Comité de sécurité (Connecting Security)	Protection de la vie privée : Groupe de travail sur la protection de la vie privée et la sécurité des Services communs d'imagerie diagnostique Sécurité : Comité de sécurité (Connecting Security)
Organisme de surveillance applicable	Protection de la vie privée : Comité directeur de ConnexionOntario Sécurité : Comité stratégique de cyberSanté Ontario	Protection de la vie privée : Comité exécutif des Services communs d'imagerie diagnostique Sécurité : Comité stratégique de cyberSanté Ontario

Tableau 1 : Organismes administratifs applicables

Terme ou acronyme	Définition
LAIPVP	*Loi de 1990 sur l'accès à l'information et la protection de la vie privée*
DRS	Dépositaire de renseignements sur la santé
LAIMPVP	*Loi de 1990 sur l'accès à l'information municipale et la*

	protection de la vie privée
RPS	Renseignements personnels sur la santé, au sens de la *Loi de 2004 sur la protection des renseignements personnels sur la santé*
LPRPS	*Loi de 2004 sur la protection des renseignements personnels sur la santé*

7 Références et documents connexes

Loi de 2004 sur la protection des renseignements personnels sur la santé (LPRPS)
Loi de 1990 sur l'accès à l'information et la protection de la vie privée (LAIPVP)
Loi de 1990 sur l'accès à l'information municipale et la protection de la vie privée (LAIMPVP)
Politique de sécurité de l'information concernant les dossiers de santé électroniques et ses procédures connexes
Politique sur la gestion de l'information et des éléments d'actif et ses procédures connexes
Politique sur les demandes de renseignements et les plaintes concernant les dossiers de santé électroniques et ses procédures connexes
Politique sur la gestion du consentement concernant les dossiers de santé électroniques et ses procédures connexes
Politique de gestion des atteintes à la confidentialité concernant les dossiers de santé électroniques et ses procédures connexes
Politique sur l'accès aux renseignements et la rectification des renseignements concernant les dossiers de santé électroniques et ses procédures connexes

8 Annexe A

Type de renseignements		Responsable
RPS figurant dans le DSE	RPS créés ou saisis dans le DSE	cyberSanté Ontario
Journaux et rapports de vérification renfermant des RPS	Cas de consultation, d'emploi ou de traitement d'une autre manière de la totalité ou d'une partie des RPS figurant dans le DSE	cyberSanté Ontario
	Cas où la totalité ou une partie des RPS figurant dans le DSE a été transmise à un DRS	cyberSanté Ontario
	Cas où la totalité ou une partie des RPS figurant dans le DSE est divulguée à un DRS et recueillie par lui par dérogation à une directive en matière de consentement	cyberSanté Ontario
	Cas où une directive en matière de consentement est donnée, retirée ou modifiée dans le DSE	cyberSanté Ontario
	Avis relatifs à la consignation et à la vérification	cyberSanté Ontario
	Rapport au CIPVP de chaque cas où la totalité ou une partie des RPS figurant dans le DSE est divulguée à un DRS et recueillie par lui par dérogation à une directive en matière de consentement	cyberSanté Ontario
	Rapports de vérification et de surveillance	DRS et cyberSanté Ontario
Copies archivées : o des RPS figurant dans le DSE; o des journaux et rapports de vérification renfermant des RPS	Copies archivées des RPS figurant de la DSE, ainsi que des journaux et rapports de vérification renfermant des RPS	cyberSanté Ontario
Copies de sauvegarde : o des RPS figurant dans le DSE; o des journaux et rapports de vérification renfermant des RPS	Copies de sauvegarde des RPS figurant dans le DSE, ainsi que des journaux et rapports de vérification renfermant des RPS	cyberSanté Ontario
Renseignements recueillis pour répondre aux demandes de particuliers concernant : o leur demande d'accès ou leur demande de rectification en vertu de la LPRPS; o leur demande visant à donner, à modifier ou à retirer une directive en matière de consentement en vertu de la LPRPS; o leur demande de renseignements ou leur plainte déposée en vertu de la LPRPS	Renseignements créés au sujet d'un particulier pour répondre à une demande d'accès, à une demande de rectification, à une demande visant à donner, à modifier ou à retirer une directive en matière de consentement en vertu de la LPRPS, ainsi qu'à une demande de renseignements ou à une plainte déposée en vertu de la LPRPS	cyberSanté Ontario ou le DRS chargé de produire le dossier
	Copies des avis envoyés aux particuliers relativement aux directives en matière de consentement	
	Avis relatifs aux demandes de directives en matière de consentement	
	Formulaire de demande d'accès (y compris les renseignements personnels et les coordonnées)	
	Avis et réponses relatifs aux demandes d'accès (y compris l'estimation des droits exigibles)	
	Demande de rectification (y compris les renseignements personnels et les coordonnées)	
	Avis et réponses relatifs aux demandes de rectification (y compris la déclaration de désaccord)	
	Plaintes et demandes de renseignements documentées (y compris les coordonnées)	
	Avis et copies des réponses aux plaintes et aux demandes de renseignements	
Renseignements créés au sujet d'un particulier dans le cadre d'une enquête sur des violations touchant la protection de la vie privée et(ou) des incidents de sécurité	Renseignements créés au sujet d'un particulier dans le cadre d'une enquête sur des violations touchant la protection de la vie privée et(ou) des incidents de sécurité	cyberSanté Ontario ou le DRS chargé de gérer l'incident

Type de renseignements		Responsable
Journaux système, journaux de suivi, rapports et documents connexes servant à l'exécution de tâches liées à la protection de la vie privée et à la sécurité, et ne renfermant pas de RPS	Journaux de diagnostics de pannes du système	cyberSanté Ontario
	Journal de tous les accès au système des DSE	cyberSanté Ontario
	Journal des activités des systèmes d'information dans le DSE	cyberSanté Ontario
	Journal de tous les accès au DSE par le DRS, ses mandataires ou fournisseurs de services électroniques	DRS
	Journal des activités des systèmes d'information dans les services d'identification et les points d'accès aux données de contribution	DRS et cyberSanté Ontario
	Journal des demandes de dérogation aux exigences en matière de sécurité de l'information	cyberSanté Ontario
	Journal des activités des administrateurs et opérateurs dans les services d'identification et les points d'accès aux données de contribution	DRS
	Journal des activités des systèmes d'information répertoriées à l'annexe A de la politique harmonisée sur la consignation et la vérification des données liées à la sécurité (*Harmonized Security Logging and Monitoring Policy*) et menées par le DRS, ses mandataires ou fournisseurs de services électroniques	cyberSanté Ontario
	Journal des activités des administrateurs de système d'information et des opérateurs de système d'information	cyberSanté Ontario
	Liste des mandataires ou des fournisseurs de services électroniques ayant autorisé l'accès aux journaux des services d'identification et des points d'accès aux données de contribution	DRS
	Liste des mandataires ou des fournisseurs de services électroniques ayant autorisé l'accès aux journaux	cyberSanté Ontario
	Journal de l'élimination des RPS figurant dans le DSE	cyberSanté Ontario
	Liste de distribution des copies de documents à diffusion restreinte	cyberSanté Ontario
	Liste des outils d'analyse des vulnérabilités et des configurations approuvés par cyberSanté Ontario	cyberSanté Ontario
	Journaux des cas où des clés, des composantes clés ou des documents connexes servant aux services d'identification et aux points d'accès aux données de contribution sont générés, retirés de leur lieu de stockage ou chargés dans un cryptographe	DRS et cyberSanté Ontario
	Journal des demandes d'identificateurs d'utilisateur administrés par les DRS et permettant l'accès aux services d'identification et à l'infrastructure de points d'accès aux données de contribution reliée au DSE	DRS
	Journal des demandes d'identificateurs gérés par cyberSanté Ontario et pouvant permettre l'accès au DSE	cyberSanté Ontario
	Liste des identificateurs ayant accès à la [solution DSE]	cyberSanté Ontario
	Journal des demandes visant à donner, à modifier ou à retirer une directive en matière de consentement (y compris les renseignements personnels et les coordonnées)	DRS et cyberSanté Ontario
	Journal attestant de la réception d'une demande de directive en matière de consentement	DRS et cyberSanté Ontario
	Journal des avis envoyés aux particuliers concernant des directives en matière de consentement	DRS et cyberSanté Ontario
	Liste des mandataires visés par une directive de consentement du mandataire	cyberSanté Ontario
	Journaux relatifs aux réponses aux demandes d'accès	DRS et cyberSanté Ontario
	Journaux relatifs aux réponses aux demandes de rectification	DRS et cyberSanté Ontario
	Historique des rectifications de dossiers de RPS figurant dans le DSE	cyberSanté Ontario

Type de renseignements		Responsable
	Avis et rapports concernant des violations touchant la protection de la vie privée ou des incidents de sécurité	cyberSanté Ontario
	Rapport d'enquête sur la gestion des violations touchant la protection de la vie privée ou rapports d'incidents de sécurité	cyberSanté Ontario
	Journal des violations touchant la protection de la vie privée	cyberSanté Ontario
	Journal des incidents de sécurité	DRS
	Rapport sur les mesures correctives face aux violations touchant la protection de la vie privée	cyberSanté Ontario
	Rapport sur l'état des mesures correctives face aux violations touchant la protection de la vie privée	cyberSanté Ontario
	Demandes de renseignements documentées (y compris les coordonnées)	cyberSanté Ontario
	Journal attestant de la réception des demandes de renseignements	cyberSanté Ontario
	Copie ou journal des réponses aux demandes de renseignements	DRS et cyberSanté Ontario
	Journal attestant de la réception des plaintes	cyberSanté Ontario
Ressources élaborées par cyberSanté Ontario dans le cadre de l'utilisation du DSE	Modèle de formation sur la protection de la vie privée et la sécurité	cyberSanté Ontario
	Modèle d'avis d'obtention du consentement	cyberSanté Ontario
Documents relatifs aux assurances	Rapport de recommandations faisant suite à l'évaluation de l'incidence sur la vie privée, et décisions et orientations connexes	cyberSanté Ontario
	Évaluation de l'incidence sur la vie privée, et décisions et orientations connexes	cyberSanté Ontario
	Évaluation des menaces et des risques (y compris les résumés)	cyberSanté Ontario
	Autoévaluation de l'état de préparation à la protection de la vie privée et à la sécurité, et décisions et orientations connexes	DRS et cyberSanté Ontario
	Autoévaluation des activités opérationnelles de protection de la vie privée et de sécurité, et décisions et orientations connexes	DRS et cyberSanté Ontario
	Plans de mesures correctives, et décisions et orientations connexes	cyberSanté Ontario
	Rapport sur l'état de la mise en œuvre des mesures correctives	cyberSanté Ontario
	Attestation de la mise en œuvre des mesures correctives	DRS et cyberSanté Ontario
	Rapports sur la non-conformité et recommandations connexes	DRS et cyberSanté Ontario
	Rapports sur la surveillance de la conformité	DRS et cyberSanté Ontario
	Rapports de vérification, et recommandations, décisions et orientations connexes	DRS et cyberSanté Ontario
	Liste des éléments d'actif dans le cadre de l'utilisation du DSE	cyberSanté Ontario
	Liste des risques – estimations des menaces et des vulnérabilités dans le cadre de l'utilisation du DSE	cyberSanté Ontario
	Modèle d'entente avec l'utilisateur final	cyberSanté Ontario
	Plan de continuité des activités	DRS et cyberSanté Ontario
Documents opérationnels de cyberSanté Ontario	Procès-verbaux des réunions du comité de protection de la vie privée et de sécurité applicable	cyberSanté Ontario