Ontario Health

Norme sur la gestion de l'information et des éléments d'actif

Version: 1.8

N° de document : 3540

Gestion du document

Fréquence de révision : Une fois par année ou selon la règle établie par le Comité ConnexionSécurité.

Historique des approbations

APPROBATEURS	DATE D'APPROBATION
Comité ConnexionSécurité	2014-09-09
Comité ConnexionSécurité	2018-03-26
Vice-présidente et chef de la sécurité	2020-03-31
Comité ConnexionSécurité	2021-03-18

Historique des révisions

NUMÉRO DE VERSION	DATE	RÉSUMÉ DES CHANGEMENTS	AUTEUR DES CHANGEMENTS
1.0	2013-12-23	Adoption de la version de novembre 2013 du groupe de travail sur la protection de la vie privée et la sécurité de ConnexionRGT.	Mark Carter
1.1	2014-08-21	Révision en fonction des commentaires reçus des membres du Comité ConnexionSécurité. Simplification de la section sur la portée; révision du point 2.7 de manière à le rendre plus clair sur la suppression de l'information; harmonisation des conditions d'application avec la politique du Comité ConnexionConfidentialité; modification de formulations dans l'annexe B pour uniformiser les définitions d'information « restreinte » et d'information « confidentielle ».	Mark Carter
1.2	2014-09-09	Révision du point 2.7 de manière à en supprimer la mention sur la réparation, car ce n'était pas applicable. Approbation de la politique à la réunion du 9 septembre 2014 du Comité ConnexionSécurité.	Mark Carter
1.3	2015-01-21	Harmonisation du nom de la politique sur le contrôle de l'accès en fonction de la décision définitive du Comité ConnexionSécurité à l'issue de la troisième étape du processus de rédaction.	Mark Carter
1.4	2015-10-19	Mise à jour des politiques pour refléter le changement de gouvernance. Le Comité directeur a été remplacé par l'organisme de surveillance compétent. Le Comité régional de protection de la vie privée et de sécurité ne participe plus au processus de décision en matière de dérogation.	Mark Carter

NUMÉRO DE VERSION	DATE	RÉSUMÉ DES CHANGEMENTS	AUTEUR DES CHANGEMENTS
1.5	2017-02-21	Mise à jour des politiques afin d'incorporer les changements mis en œuvre lors du rafraîchissement 2017. La définition de « solution de DSE » a été ajustée. Plusieurs contrôles ont été reformulés afin d'inclure « participant » dans la solution de DSE.	Ravi Addepalli
1.6	16 mars 2018	Mise à jour de la norme afin d'inclure l'accès au DSE par les patients.	Geovanny Diaz
1.7	31 mars 2020	Mise à jour la norme dans un nouveau modèle et fair des révisions mineures pour plus de clarté. Mise à jour la norme dans un nouveau modèle et fair des révisions mineures pour plus de clarté.	John Limarzi
1.8	2021-04-01	Examen du document avec des modifications mineures, mise à jour du cycle de révision tous les deux ans	Ana Fukushima

Norme sur la gestion de l'information et des éléments d'actif

Objet

La présente norme vise à définir les contrôles nécessaires pour protéger l'information et le matériel constituant les technologies de l'information (les « éléments d'actif »).

Portée

La présente norme s'applique aux entités suivantes :

- l'équipe de [la solution de DSE] et [la solution de DSE], , y compris la totalité des portails et des applications pour les patients;

- les dépositaires de renseignements sur la santé, leurs mandataires et leurs fournisseurs de services électroniques qui créent, versent et consultent des données dans [la solution de DSE] ou qui accèdent à cette dernière.

La politique ne s'applique pas aux entités suivantes :

les DRS, leurs mandataires et leurs fournisseurs de services électroniques qui ne créent pas, ne versent pas et ne consultent pas de données dans [la solution de DSE] et qui n'accèdent pas à cette dernière.

Définitions

[la solution de DSE] : Solution utilisée, y compris les systèmes connexes, pour stocker et rendre accessibles les renseignements personnels sur la santé contenus dans les systèmes de renseignements électroniques sur la santé des dépositaires de renseignements sur la santé.

[La solution de DSE] inclut les portails et les applications pour les patients (affiliés ou non à un dépositaire de renseignements sur la santé) qui facilitent l'accès du patient au DSE. Ces applications peuvent être :

- Commandées par le fournisseur (le fournisseur facilite la communication avec le patient)
- Fournies directement au patient (le patient a un accès direct au DSE)
- Commandées par le patient (le patient délègue l'accès à un mandataire spécial ou à d'autres délégués, p. ex., un membre de la famille ou un médecin).

Équipe de [la solution de DSE] : également appelée bureau de l'équipe; comprend des agents et des fournisseurs de services électroniques qui soutiennent [la solution de DSE], y compris les activités, les initiatives et les processus associés à la protection de la vie privée et à la sécurité.

À double emballage : Se dit d'un élément dans une enveloppe ou un contenant qu'on place à l'intérieur d'une autre enveloppe ou d'un autre contenant, habituellement pour le transport physique de documents sur papier ou d'éléments d'actif.

Connaissance répartie : Principe exigeant le traitement de l'information sous forme d'éléments distincts du moment de la production de l'information jusqu'à la combinaison des éléments en vue de leur utilisation. Un élément à lui seul ne permet pas de décoder le message.

Devrait/devraient : S'utilisent lorsqu'il y a des raisons, selon les circonstances, de ne pas exécuter ce qui est proposé. La personne doit cependant comprendre les conséquences de ses actes si elle décide de ne pas adhérer à ce qui est écrit et songer à mettre en œuvre des mesures de contrôle en guise de compensation.

Doit/doivent : S'utilisent dans le cas des exigences absolues où il n'y a aucune autre option possible.

Double contrôle : Principe de contrôle exigeant l'apport de deux personnes pour effectuer une tâche donnée.

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.

Organisme de surveillance compétent : L'organisme de surveillance compétent est formé de cadres supérieurs qui supervisent tous les aspects de la [solution DSE]. Voir la section intitulée Structure de la politique de gouvernance dans le document Politique de sécurité de l'information.

Peut/peuvent : S'utilisent lorsque ce qui est proposé n'est qu'une recommandation ou ne sert que d'exemple qui ne se veut pas exhaustif.

Service de gestion d'identité : Technologies et services, politiques, processus et procédures connexes servant à créer, à conserver, à mettre en sécurité, à valider, à affirmer et à gérer des identités électroniques pour [la solution de DSE].

Technologie de l'information : Tout élément (matériel ou électronique) utilisé pour l'acquisition, le stockage, la manipulation, la gestion, le déplacement, le contrôle, l'affichage, l'échange, l'envoi ou la réception automatiques de données ou d'information. Comprend, sans s'y limiter, le matériel informatique, les logiciels, les microprogrammes, le matériel auxiliaire et les ressources connexes.

Terminal d'envoi de données : Technologies et processus connexes qui alimentent le dépôt de données cliniques et font l'objet des recherches de données par l'utilisateur en milieu clinique. Comprend habituellement le système d'information (système d'information hospitalier, système d'information de laboratoire, système d'information clinique, etc.) qui se branche automatiquement à [la solution de DSE] pour rendre les données cliniques accessibles.

Exigences de la norme

1. Exigences pour les dépositaires de renseignements sur la santé

1.1. Les dépositaires de renseignements sur la santé (DRS) doivent veiller à ce que tous les renseignements personnels sur la santé (RPS) transmis au bureau de l'équipe de [la solution de DSE] ou à [la solution de DSE] le soient de manière sécuritaire, c'est-à-dire par messagerie électronique sécurisée, chiffrement ou réseau privé virtuel.

2. Exigences pour l'équipe de [la solution de DSE]

2.1. L'équipe de [la solution de DSE] doit mettre en œuvre et conserver un schéma de classification de l'information et des éléments d'actif visant à assurer la confidentialité, l'accessibilité et l'intégrité de l'information et des éléments d'actif qu'elle possède ou gère. Consultez à cet effet l'annexe A intitulée *Schéma de classification de l'information et des éléments d'actif*.

Nom

2.2. L'équipe de [la solution de DSE] doit nommer l'information et les éléments d'actif conformément aux exigences suivantes :

Type de support	**Public**	**Interne**	**Confidentiel**	**RPS**	**Restreint**
Document papier	Facultatif		Nom à inclure sur la première page et sur chaque page subséquente.		
Électronique	Facultatif		Nom à inclure sur la première page et sur chaque page subséquente de tout fichier qui peut être imprimé (capture d'écran, PDF, traitement de texte Word, feuille de calcul, présentation sur diapositives, etc.).		
Courriel	Facultatif		Nom à inclure dans le corps du texte ou dans la ligne de l'objet.		
Dispositif portatif ou amovible	Facultatif				
Dispositif de stockage intégré	Facultatif				

2.3. Même si ce n'est pas obligatoire, l'équipe de [la solution de DSE] peut nommer l'information ou les éléments d'actif d'après la catégorie d'intégrité et d'accessibilité qui leur a été accordée.

Exigences de protection générales

2.4. L'équipe de [la solution de DSE] doit veiller à ce que tous les RPS et les éléments d'actif qui traitent ou stockent des RPS soient protégés, au minimum, conformément au contenu de l'annexe B intitulé *Exigences de protection de l'information et des éléments d'actif*. L'équipe de [la solution de DSE] peut choisir d'appliquer des mesures de contrôle qui s'ajoutent à celles requises à l'annexe B.

2.5. Lorsque de l'information est combinée à de l'information de classe inférieure, l'équipe de [la solution de DSE] doit veiller à ce que ce soit l'information ayant la classe la plus élevée qui détermine la classe minimale de toute l'information réunie.

Exigences générales de protection

2.6. L'équipe de [la solution de DSE] doit veiller à ce que tous les exemplaires papier contenant de l'information considérée comme restreinte soient munis d'un numéro unique au moment de leur création et à ce qu'on conserve une liste de contrôle contenant chaque exemplaire numéroté ainsi que la personne à qui il est destiné.

2.7. L'équipe de [la solution de DSE] doit retirer toute l'information (les RPS et l'information dans [la solution de DSE]) classée comme interne ou de niveau supérieur des dispositifs de stockage intégré et des supports amovibles avant tout envoi externe. Le retrait de l'information classée comme confidentielle ou de niveau supérieur doit se faire de manière à ce que l'information ne puisse être obtenue ou consultée.

2.8. La solution de DSE: Le programme doit s'assurer que toutes les copies en papier des documents classés comme restreints doivent être numérotées individuellement au moment de la création et qu'une liste principale associant chaque copie numérotée à la personne à qui elle a été distribuée est maintenue.

2.9. La solution de DSE: Le programme doit supprimer toutes les informations (PHI et [la solution EHR] classées comme internes ou superieur des périphériques de stockage intégrés et des supports amovibles avant d'être envoyées à l'externe. La suppression des informtations classés confidentiels ou supérieur doit être effectuée de manière à ce que les informations ne puissent pas être récupérés et vus.

2.10. L'équipe de [la solution de DSE] doit journaliser la destruction des RPS et du dépôt de données cliniques de [la solution de DSE] le plus tôt possible, mais pas plus de cinq jours après la destruction. Le journal doit au minimum contenir les éléments suivants :

2.10.1. la date de destruction des RPS;

2.10.2. la description de l'étendue des RPS détruits;

2.10.3. la description du mode de destruction des RPS;

2.10.4. l'identité de la personne qui a détruit les RPS;

2.10.5. l'identité de la personne qui a autorisé la destruction des RPS.

Dérogations Toute dérogation à la norme doit être approuvée par l'organisme de surveillance compétent, lequel l'autorisera uniquement lorsque la situation le justifie et au degré minimal nécessaire pour la justification apportée.

Consultez à cet effet l'annexe A intitulée *Demandes de dérogation aux exigences en matière de sécurité de l'information* dans la Politique de sécurité de l'information.

Application Tous les cas de non-respect seront examinés par l'organisme de surveillance compétent.

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

Références

Lois

- LPRPS, art. 12 et 13 et partie V.1
- O. Reg. 329/04, art. 6

Normes internationales

- ISO/IEC 27001:2013, Information Technology – Security Techniques – Information Security Management Systems – Requirements
- ISO/IEC 27002:2013, Information Technology – Security Techniques – Code of Practice for Information Security Management
- ISO/IEC 27005: 2018 Information Technology – Security Techniques – Information Security Risk Management

Documents de politiques et de normes sur les DSE de Santé Ontario

- Information Security Policy
- Acceptable Use of Information and Information Technology Standard
- Access Control and Identity Management Standard for System Level Access
- Local Registration Authority Procedures Standard
- Identity Federation Standard
- Business Continuity Standard
- Cryptography Standard
- Electronic Service Providers Standard
- Information Security Incident Management Standard
- Information and Asset Management Standard
- Network and Operations Standard
- Security Logging and Monitoring Standard
- Systems Development Lifecycle Standard
- Physical Security Standard
- Threat Risk Management Standard

Référence à Inforoute Santé du Canada

- Exigences en matière de protection de la confidentialité et de sécurité d'Inforoute Santé du Canada (version 1.1 révisée le 7 février 2005)

Autre

- Directives concernant la sécurité des transmissions par télécopieur du commissaire à l'information et à la protection de la vie privée de l'Ontario (janvier 2003)

Annexe A : Schéma de classification de l'information et des éléments d'actif

Classes		Description	Exemples d'information ou d'éléments d'actif	Exemples de conséquences des risques
Confidentialité	**Intégrité et accessibilité**			
Public	**FAIBLE**	Information ou éléments d'actif qui sont utilisés dans le cours normal des activités et qui n'ont pas vraiment de risques de causer des préjudices. **Accessible au public.**	• L'information se trouve sur le site Web externe de l'équipe de [la solution de DSE]. • Offres d'emploi externes.	• Aucun effet si l'information est rendue publique. • La perte de l'information n'entraînerait pas de préjudices à des patients; à l'équipe [la solution de DSE], à ses mandataires ou à ses fournisseurs de services électroniques ou aux DRS, à leurs mandataires ou à leurs fournisseurs de services électroniques. • La perte d'intégrité ou d'accessibilité de l'information n'a pas d'effet négatif sur les patients; l'équipe [la solution de DSE], ses mandataires ou ses fournisseurs de services électroniques ou les DRS, leurs mandataires ou leurs fournisseurs de services électroniques.
Interne		Information ou éléments d'actif qui ont un degré de sensibilité peu élevé à l'extérieur de [la solution de DSE] et qui pourraient avoir des effets de faible ampleur sur les niveaux de service ou la performance ou entraîner des pertes financières peu importantes. **L'information est accessible aux mandataires de [la solution de DSE], aux fournisseurs de services électroniques de [la solution de DSE] et aux DRS qui en ont besoin.**	• Modes d'emploi des applications de [la solution de DSE]. • Documents de planification généraux concernant [la solution de DSE]. • Renseignements généraux de nature financière concernant le fonctionnement de [la solution de DSE].	• Faible degré de risque si l'information est rendue publique. • La perte d'intégrité ou d'accessibilité de l'information pourrait avoir un effet négatif minime sur des patients; l'équipe [la solution de DSE], ses mandataires ou ses fournisseurs de services électroniques ou les DRS, leurs mandataires ou leurs fournisseurs de services électroniques.

Confidentiel	**MOYEN**	Information ou éléments d'actif qui ont un degré de sensibilité moyen à élevé dans [la solution de DSE] et à l'extérieur de cette dernière et qui pourraient avoir des effets de moyenne ampleur sur les niveaux de service ou la performance ou entraîner des pertes financières moyennement importantes. **L'information n'est accessible qu'à des groupes ou à des postes ayant une fonction particulière pour [la solution de DSE], ses mandataires ou ses fournisseurs de services électroniques ou les DRS, leurs mandataires ou leurs fournisseurs de services électroniques.**	• Renseignements personnels (exclut les RPS), par exemple le taux de rémunération d'un mandataire identifiable. • Information visée par des ententes de non-divulgation. • Transactions financières n'incluant pas des RPS ou de l'information restreinte. • Documents décrivant en détail l'architecture du réseau.	• Atteinte à la réputation. • Perte de confiance à l'égard de l'équipe de [la solution de DSE]. • Atteinte à la vie privée. • Perte de secrets commerciaux ou de propriété intellectuelle. • La perte d'intégrité ou d'accessibilité de l'information pourrait avoir un effet négatif moyen sur des patients; l'équipe [la solution de DSE], ses mandataires ou ses fournisseurs de services électroniques ou les DRS, leurs mandataires ou leurs fournisseurs de services électroniques.
RPS	**ÉLEVÉ**	Tous les RPS. **L'information n'est accessible qu'à des groupes ou à des postes ayant une fonction particulière pour [la solution de DSE], ses mandataires ou ses fournisseurs de services électroniques ou les DRS, leurs mandataires ou leurs fournisseurs de services électroniques.**	• RPS.	• Atteinte à la réputation. • Perte de la confidentialité des renseignements personnels sur la santé. • Perte de confiance à l'égard de l'équipe de [la solution de DSE]. • La perte d'intégrité ou d'accessibilité de l'information pourrait avoir un effet négatif moyen à élevé sur un patient; l'équipe [la solution de DSE], ses mandataires ou ses fournisseurs de services électroniques ou les DRS, leurs mandataires ou leurs fournisseurs de services électroniques.

Restreint	**CRITIQUE**	Information ou éléments d'actif qui ont un degré extrêmement élevé de sensibilité à l'intérieur et à l'extérieur de [la solution de DSE] et qui pourraient avoir des effets de grande ampleur sur les niveaux de service ou la performance ou entraîner des pertes financières très importantes. **Information accessible seulement à des personnes nommées ou à des postes précis (par exemple Jean Untel ou le vice-président des opérations) pour [la solution de DSE], ses mandataires ou ses fournisseurs de services électroniques ou les DRS, leurs mandataires ou leurs fournisseurs de services électroniques.**	• Clés cryptographiques. • Mots de passe. • Modules de sécurité matériels.	• Atteinte à la réputation. • Retombées financières importantes. • Perte importante de la confidentialité des renseignements personnels sur la santé. • Perte de confiance à l'égard de l'équipe de [la solution de DSE]. • Ruptures de partenariats et de relations. • La perte d'intégrité ou d'accessibilité de l'information pourrait avoir un effet négatif élevé à extrême sur des patients; l'équipe [la solution de DSE], ses mandataires ou ses fournisseurs de services électroniques ou les DRS, leurs mandataires ou leurs fournisseurs de services électroniques.

Annexe B : Exigences de protection de l'information et des éléments d'actif

Exigences relatives au stockage

Type d'information ou d'élément d'actif	Public	Interne	Confidentiel	RPS	Restreint
Document papier	Aucune exigence spéciale en matière de confidentialité, d'intégrité ou d'accessibilité.	Dans un contenant sous verrou laissé sans surveillance dans un endroit où a accès le public. – OU – Dans une zone où seuls l'équipe de [la solution de DSE], ses mandataires ou ses fournisseurs de services électroniques ont accès.	Dans un contenant sous verrou si laissé sans surveillance dans un endroit où ont accès le public ou des personnes non autorisées. – OU – Dans une zone à accès restreint où toutes les personnes ayant droit d'accès ont l'autorisation de voir l'information.	Dans un contenant sous verrou si laissé sans surveillance dans un endroit où ont accès le public ou des personnes non autorisées. – OU – Dans une zone à accès restreint où toutes les personnes ayant droit d'accès ont l'autorisation de voir l'information.	Stocké selon les principes de double contrôle et de connaissance répartie. Recours à un journal d'audit de sécurité pour tout accès physique (par exemple, un journal des signatures pour chaque fois où une personne accède à l'information). Doit être stocké dans une zone à accès restreint ET verrouillé dans un contenant.
Électronique	Aucune exigence spéciale en matière de confidentialité, d'intégrité ou d'accessibilité.	Doit être stocké sur un réseau interne ou un dispositif de stockage.	Doit être stocké sur un dispositif chiffré. – OU – Stocké sur un réseau interne muni de mesures de sécurité logiques pour empêcher tout accès non autorisé.	Doit être stocké sur un dispositif chiffré, et seuls les RPS nécessaires doivent être stockés. – OU – Stocké sur un réseau interne chiffré muni de mesures de sécurité logiques, et physiques si la situation s'y prête, pour empêcher tout accès non autorisé.	Doit être stocké sur un dispositif chiffré, et seule l'information restreinte nécessaire doit être stockée. – OU – Stocké sur un réseau interne chiffré muni de mesures de sécurité logiques, et physiques si la situation s'y prête, pour empêcher tout accès non autorisé.

Dispositif portatif ou amovible	Aucune exigence spéciale en matière de confidentialité, d'intégrité ou d'accessibilité.	Doit être stocké dans une zone à accès restreint.	Doit être chiffré. Doit être dans un contenant sous verrou dans une zone à accès restreint s'il n'y a pas de supervision ou si on ne s'en sert pas.	Doit être chiffré. Doit être dans un contenant sous verrou dans une zone à accès restreint s'il n'y a pas de supervision ou si on ne s'en sert pas.	Doit être chiffré. Doit être stocké dans une zone à accès restreint ET verrouillé dans un contenant s'il n'y a pas de supervision ou si on ne s'en sert pas. • Devrait être stocké selon le principe de double contrôle. Recours à un journal d'audit de sécurité pour tout accès physique au dispositif.
Dispositif de stockage intégré	Doit être stocké dans une zone à accès restreint. Des sauvegardes régulières devraient être effectuées pour assurer l'accessibilité et l'intégrité du dispositif.	Doit être stocké dans une zone à accès restreint. Des sauvegardes régulières devraient être effectuées pour assurer l'accessibilité et l'intégrité du dispositif.	Devrait être chiffré. Doit être stocké dans une zone à accès restreint. Des sauvegardes régulières doivent être effectuées pour assurer l'accessibilité et l'intégrité du dispositif.	Doit être chiffré. Doit être stocké dans une zone à accès restreint. Des sauvegardes régulières doivent être effectuées pour assurer l'accessibilité et l'intégrité du dispositif.	Doit être chiffré. Doit être stocké dans une zone à accès restreint hautement sécurisée. Doit avoir recours à un journal d'audit de sécurité pour tout accès physique au dispositif. Des sauvegardes régulières doivent être effectuées pour assurer l'accessibilité et l'intégrité du dispositif.

Exigences relatives à la transmission et au transport

Type d'information ou d'élément d'actif	Public	Interne	Confidentiel	RPS	Restreint
Document papier *(Fait référence au transport physique de documents papier.)*	Aucune exigence spéciale.		<u>À l'interne (même lieu)</u> • Doit être placé dans une enveloppe ou un contenant opaque scellé portant une étiquette indiquant la catégorie d'information. <u>À l'interne (lieu différent)</u> • Doit être placé dans une enveloppe ou un contenant opaque scellé portant une étiquette indiquant la catégorie d'information. • Doit être à double emballage dans une enveloppe ou un contenant opaque scellé. L'enveloppe extérieure ne doit pas porter la mention de la catégorie d'information. • Doit exiger la signature du destinataire.		<u>À l'interne (même lieu)</u> • Doit être placé dans une enveloppe ou un contenant opaque scellé inviolable portant une étiquette indiquant la catégorie d'information. <u>À l'interne (lieu différent) et à l'externe</u> • Doit être placé dans une enveloppe ou un contenant opaque scellé inviolable portant une étiquette indiquant la catégorie d'information. • Doit être à double emballage dans une enveloppe opaque scellée inviolable. L'enveloppe extérieure ne doit pas porter la mention de la catégorie d'information. • Doit exiger la signature du destinataire. • Si envoyé par la poste, doit l'être par service de messagerie sécurisé. • Si transporté par les mandataires ou les fournisseurs de services électroniques de l'équipe de [la solution de DSE] ou les DRS, leurs mandataires ou leurs fournisseurs de services électroniques, doit demeurer en double garde.
Électronique *(Fait référence à la transmission électronique de l'information.)*			Doit être envoyé par voie sécurisée.		

Type d'information ou d'élément d'actif	Public	Interne	Confidentiel	RPS	Restreint
Dispositif portatif ou amovible *(Fait référence au transport physique du dispositif.)*			<u>À l'interne (même lieu)</u> • Doit être placé dans une enveloppe ou un contenant opaque scellé portant une étiquette indiquant la catégorie d'information. <u>À l'interne (lieu différent) et à l'externe</u> • Doit être placé dans une enveloppe ou un contenant opaque scellé portant une étiquette indiquant la catégorie d'information. • Doit être à double emballage dans une enveloppe ou un contenant opaque scellé. L'enveloppe ou le contenant extérieur ne doit pas porter la mention de la catégorie d'information. • Doit exiger la signature du destinataire.		<u>À l'interne (même lieu)</u> • Doit être placé dans une enveloppe ou un contenant opaque scellé inviolable portant une étiquette indiquant la catégorie d'information. <u>À l'interne (lieu différent) et à l'externe</u> • Doit être placé dans une enveloppe ou un contenant opaque scellé inviolable portant une étiquette indiquant la catégorie d'information. • Doit être à double emballage dans une enveloppe ou un contenant scellé inviolable. L'enveloppe ou le contenant extérieur ne doit pas porter la mention de la catégorie d'information. • Doit exiger la signature du destinataire. • Si envoyé par la poste, doit l'être par service de messagerie sécurisé. • Si transporté par les mandataires ou les fournisseurs de services électroniques de l'équipe de [la solution de DSE] ou les DRS, leurs mandataires ou leurs fournisseurs de services électroniques, doit demeurer en double garde.
Dispositif de stockage intégré *(Fait référence au transport physique du dispositif.)*					

Exigences relatives à l'élimination ou à la destruction de l'information

Type d'information ou d'élément d'actif	Public	Interne	Confidentiel	RPS	Restreint
Document papier	Aucune exigence spéciale.	Déchiqueté à l'aide d'une déchiqueteuse avec coupe en travers ou placé dans une poubelle sécurisée avant d'être déchiqueté à l'aide d'une déchiqueteuse avec coupe en travers ou brûlé par un mandataire ou un fournisseur de services électroniques désigné.	Déchiqueté à l'aide d'une déchiqueteuse avec coupe en travers ou placé dans une poubelle sécurisée avant d'être déchiqueté à l'aide d'une déchiqueteuse avec coupe en travers ou brûlé par un mandataire ou un fournisseur de services électroniques désigné.	Déchiqueté à l'aide d'une déchiqueteuse avec coupe en travers ou placé dans une poubelle sécurisée avant d'être déchiqueté à l'aide d'une déchiqueteuse avec coupe en travers ou brûlé par un mandataire ou un fournisseur de services électroniques désigné.	Doit être brûlé sur place en suivant le principe de double contrôle. – OU – Doit être déchiqueté à l'aide d'une déchiqueteuse avec coupe en travers ET placé dans une poubelle sécurisée désignée avant d'être déchiqueté à l'aide d'une déchiqueteuse avec coupe en travers ou brûlé par un mandataire ou un fournisseur de services électroniques désigné.
Électronique	Aucune exigence spéciale.	Supprimer l'information.	Supprimer l'information stockée sur le dispositif chiffré ou le réseau de stockage interne. Il est possible de déchiqueter les CD et DVD à l'aide d'une déchiqueteuse avec coupe en travers ou de les placer dans une poubelle sécurisée avant de les faire déchiqueter à l'aide d'une déchiqueteuse avec	Supprimer l'information stockée sur le dispositif chiffré ou le réseau de stockage interne chiffré. Il est possible de déchiqueter les CD et DVD à l'aide d'une déchiqueteuse avec coupe en travers ou de les placer dans une poubelle sécurisée avant de les faire déchiqueter à l'aide d'une déchiqueteuse avec	Doit être supprimée ou écrasée de manière sécuritaire qui rend impossible la récupération de l'information.

Type d'information ou d'élément d'actif	Public	Interne	Confidentiel	RPS	Restreint
			coupe en travers ou de les faire brûler par un mandataire ou un fournisseur de services électroniques désigné.	coupe en travers ou de les faire brûler par un mandataire ou un fournisseur de services électroniques désigné.	
Dispositif portatif ou amovible **Dispositif de stockage intégré**	Aucune exigence spéciale.	Supprimer tous les fichiers.	Doit être supprimé ou écrasé de manière sécuritaire qui rend impossible la récupération de l'information. – OU – Doit être physiquement détruit d'une manière qui rend impossible la récupération de l'information.	Doit être supprimé ou écrasé de manière sécuritaire qui rend impossible la récupération de l'information. – OU – Doit être physiquement détruit d'une manière qui rend impossible la récupération de l'information. La destruction de RPS dans le dépôt de données cliniques doit être inscrite dans un journal (voir le point 2.8).	<u>Dispositifs contenant des clés cryptographiques</u> : • Doit être physiquement détruit d'une manière qui rend impossible la récupération de l'information. <u>Tous les autres dispositifs</u> : • Doit être supprimé ou écrasé de manière sécuritaire qui rend impossible la récupération de l'information ou physiquement détruit de manière qui rend impossible la récupération de l'information.