Ontario Health

# Norme sur la journalisation de sécurité et la surveillance

Version: 2.0

N° de document : 3542

## 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 | 2017-03-20 |
| Comité ConnexionSécurité | 2018-03-26 |
| 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 | 2014-10-09 | Révision en fonction des commentaires reçus de responsables des programmes ConnexionRGT et Connexion Sud-Ouest de l'Ontario et du groupe de protection des renseignements personnels sur la santé. Harmonisation des sections de la portée, des dérogations et de l'application avec les politiques du Comité ConnexionConfidentialité. Clarification de la distinction entre les politiques sur la sécurité et la protection de la vie privée (système et application); suppression du point 1.24 lié à la conservation en raison de son ambiguïté et du double emploi avec le point 1.23. | Mark Carter |
| 1.2 | 2014-10-17 | Révision à la suite de la réunion du Comité ConnexionSécurité du 15 octobre. Ajout, au point 1.23, d'une référence à la norme pour les fournisseurs d'identité et la politique sur la conservation de données du Comité ConnexionConfidentialité. Révision de l'annexe A par l'ajout du contenu requis dans les services de gestion d'identité et les terminaux d'envoi de données. | Mark Carter |
| 1.3 | 2014-10-28 | Révision en fonction des commentaires du Comité Connexion Nord et Est de l'Ontario et des discussions avec les membres. | Mark Carter |
| 1.4 | 2014-11-26 | Révision à la suite de la réunion du Comité ConnexionSécurité du 26 novembre. Ajout de l'exigence d'examiner les journaux chaque trimestre au point 1.20. | Mark Carter |

| NUMÉRO DE VERSION | DATE | RÉSUMÉ DES CHANGEMENTS | AUTEUR DES CHANGEMENTS |
|---|---|---|---|
| | | Suppression des périodes de conservation des journaux indiquées et remplacement par une référence à la politique sur la conservation de données du Comité ConnexionConfidentialité. Approbation de la politique à la réunion. | |
| 1.5 | 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 |
| 1.6 | 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 |
| 1.7 | 2017-03-20 | Mise à jour de la norme afin de refléter l'ITSM. Changement du titre du document, qui passe de « Politique » à « Norme ». Mise à jour de la définition de « la solution de DSE ». Révision des contrôles en fonction des commentaires. | Raviteja Addepalli |
| 1.8 | 2018-03-16 | Mise à jour de la norme afin d'inclure l'accès au DSE par les patients. | Geovanny Diaz |
| 2.0 | 2021-04-01 | Examen du document avec des modifications mineures et mise à jour du cycle de révision tous les deux ans | Ana Fukushima |

# Norme sur la journalisation de sécurité et la surveillance

## Objet

La présente norme a pour but de définir les exigences de journalisation et de surveillance des événements à l'échelle des systèmes dans [la solution de DSE] ainsi que les services de gestion d'identité, les terminaux d'envoi de données et l'infrastructure d'appui des dépositaires de renseignements sur la santé (DRS).

## Portée

La présente norme s'applique à [la solution de DSE] et à l'équipe qui en est responsable, y compris la totalité des portails et des applications pour les patients, dans le cas de la journalisation à l'échelle des systèmes comme le définit l'annexe A intitulée *Sources et contenu des journaux*.

Elle vise les éléments suivants dans le cas des DRS qui utilisent [la solution de DSE] pour voir, traiter ou autrement manipuler des renseignements personnels sur la santé (RPS) à l'aide d'une **technologie de gestion d'identité locale** :

- le système de contrôle de l'accès et de gestion d'identité du DRS (les « services de gestion d'identité ») qui gère les processus d'authentification et d'autorisation donnant accès à [la solution de DSE] (solution de service d'émission de jetons de sécurité de [la solution de DSE], Active Directory Federation Services 2.0 de Microsoft ou autre);

- toute connexion directe au portail du fournisseur de [la solution de DSE] et aux fonctions administratives de cette dernière, ce qui comprend les composants connectés (pare-feu, serveur mandataire, etc.);

- l'intégration du portail du fournisseur de [la solution de DSE] au système d'information local du DRS ou à l'application de gestion des dossiers médicaux électroniques.

Elle vise plutôt les éléments suivants dans le cas des DRS qui utilisent [la solution de DSE] pour voir, traiter ou autrement manipuler des RPS à l'aide du **service ONE ID de Santé Ontario** :

- toute connexion directe aux fonctions administratives de [la solution de DSE], ce qui comprend les composants connectés (pare-feu, serveur mandataire, etc.).

Dans le cas des DRS qui créent et versent des RPS dans le dépôt de données cliniques de [la solution de DSE], la présente norme, en plus de ce qui est prévu pour les sites qui ne font que consulter les données, s'applique aux éléments suivants :

- les terminaux d'envoi de données qui fournissent des RPS au dépôt de données cliniques de [la solution de DSE];

- les technologies de l'information et les processus qui assurent la qualité des données envoyées (la mise en correspondance de la terminologie, par exemple).

Consultez la politique harmonisée sur la journalisation et l'audit chaque fois que survient l'une ou l'autre des situations suivantes :

- les RPS dans [la solution de DSE] sont consultés, traités ou manipulés d'une quelconque autre façon en partie ou en entier[1];

- les RPS dans [la solution de DSE] sont transférés en partie ou en entier à un DRS;

- les RPS dans [la solution de DSE] sont divulgués à un DRS ou recueillis par un DRS en partie ou en entier à la suite d'une dérogation à une directive sur le consentement;

- une directive sur le consentement est formulée, modifiée ou retirée dans [la solution de DSE].

La norme ne s'applique pas aux DRS, à leurs mandataires et à 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.

[1] Aux fins de clarté, la phrase ainsi formulée comprend la collecte, l'utilisation et la divulgation des renseignements le cas échéant.

# 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.

**Audit :** Fait d'inspecter les journaux dans les buts suivants :

- vérifier l'activité qui a eu lieu dans un système d'information ou dans un réseau par tout mandataire ou fournisseur de services électroniques de l'équipe de [la solution de DSE] ou tout mandataire ou fournisseur de services électroniques d'un dépositaire de renseignements sur la santé;

- vérifier si un système d'information est en bon état;

- répondre aux questions sur les raisons pour lesquelles un système d'information est parvenu à un état donné.

**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.

**Fournisseur de services électroniques :** Personne ou entité 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.

**Journal d'audit :** Série chronologique de journaux relevant les activités dans un système d'information et les activités d'un dépositaire de renseignements sur la santé, d'un mandataire ou d'un fournisseur de services électroniques. On peut ainsi reconstituer les événements passés, faire le suivi des activités qui ont eu lieu et possiblement détecter et identifier les intrus.

**Journal :** Relevé des événements qui ont leu dans [la solution de DSE] ou dans les systèmes d'information et les réseaux du dépositaire de renseignements sur la santé.

**Journalisation :** Processus de relevé d'un ensemble prédéfini d'activités dans un système d'information ou un réseau de DRS, de mandataire ou de fournisseur de services électroniques. Les processus de journalisation automatique servent à établir les journaux d'audit des activités et des événements ayant lieu dans un système d'information.

**Organisme de surveillance compétent :** L'organisme de surveillance compétent est formé de cadres supérieurs qui supervisent tous les aspects liés à 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].

**Surveillance :** Processus d'observation, de supervision ou de contrôle des activités dans un système d'information ou un réseau.

**Système d'information :** Ensemble autonome de technologies de l'information organisées de manière à recueillir, à traiter, à conserver, à utiliser, à divulguer, à détruire ou à éliminer l'information.

**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, moteur d'interface HL7, etc.) qui se branche automatiquement à [la solution de DSE] pour rendre les données cliniques accessibles.

# Exigences de la politique

## 1. Exigences pour les dépositaires de renseignements sur la santé

1.1. Les DRS doivent journaliser tous les cas d'accès à [la solution de DSE] par les DRS, leurs mandataires et leurs fournisseurs de services électroniques ainsi que les activités dans leurs services de gestion d'identité et leurs terminaux d'envoi de données.

1.2. Les DRS devraient classer et protéger les journaux en fonction du plus haut degré d'importance des renseignements qui se trouvent dans les terminaux d'envoi de données et les services de gestion d'identité.

**Création de journaux**

1.3. Les DRS doivent journaliser toutes les activités des administrateurs et des opérateurs dans leurs services de gestion d'identité et leurs terminaux d'envoi de données dans le cadre du processus de création du journal d'audit.

1.4. Les DRS doivent veiller à ce que les journaux des terminaux d'envoi de données et des services de gestion d'identité contiennent au minimum les renseignements suivants pour chaque activité (il faut consulter la norme sur le fournisseur d'identité pour voir les exigences de journalisation précises relatives aux fonctions des services de gestion d'identité comme l'enregistrement et l'authentification) :

1.4.1. les identifiants (le plus possible d'entre eux) de l'entité qui demande l'action (nom d'utilisateur, nom de l'ordinateur, adresse IP et adresse MAC, par exemple);

1.4.2. les identifiants (le plus possible d'entre eux) de l'objet dans lequel a été accomplie l'action (nom des fichiers, identifiants uniques des registres consultés dans une base de données, adresse IP et adresse MAC, par exemple);

1.4.3. la date et l'heure;

1.4.4. l'activité comme telle (ouverture ou fermeture de session, par exemple);

1.4.5. l'état de l'activité (accès accordé ou refusé, par exemple);

1.4.6. le type d'accès (lecture seule, écriture, exécution);

1.4.7. les alertes envoyées par les systèmes de contrôle de l'accès et de surveillance du réseau.

1.5. Les DRS doivent filtrer les journaux de leurs services de gestion d'identité et de leurs terminaux d'envoi de données à la source.

1.6. Les DRS doivent synchroniser l'horloge de leurs services de gestion d'identité et de leurs terminaux d'envoi de données avec une horloge centralisée. Les DRS doivent valider la synchronisation des horloges au moins une fois par jour pour que les horloges indiquent toujours la même heure entre elles.

**Protection des journaux**

1.7. Les DRS doivent implanter des mesures de contrôle visant à protéger la confidentialité et l'intégrité des journaux de leurs services de gestion d'identité et de leurs terminaux d'envoi de données pendant leur entreposage et leur transmission.

1.8. Les DRS doivent restreindre l'accès aux journaux des services de gestion d'identité et des terminaux d'envoi de données.

1.9. Les DRS devraient conserver une liste de tous les mandataires ou fournisseurs de services électroniques qui ont l'autorisation d'accéder aux journaux des services de gestion d'identité et des terminaux d'envoi de données. La liste devrait contenir les éléments suivants :

1.9.1. le nom complet du mandataire ou du fournisseur de services électroniques;

1.9.2. l'identifiant qu'a utilisé le mandataire ou le fournisseur de services électroniques pour l'accès logique au journal;

1.9.3. le nom du journal (ainsi que son type) auquel a accès le mandataire ou le fournisseur de services électroniques.

1.10. Les DRS ne devraient pas configurer les journaux de leurs services de gestion d'identité et de leurs terminaux d'envoi de données de telle manière que les anciennes données sont écrasées lorsque la limite de taille du journal est atteinte.

1.11. Les DRS devraient interdire à leurs mandataires et à leurs fournisseurs de services électroniques ayant accès aux journaux de leurs services de gestion d'identité et de leurs terminaux d'envoi de données de supprimer ou de désactiver les journaux de leurs propres activités.

1.12. Les DRS devraient veiller à ce que les activités de gestion des sources de création de journaux pour leurs services de gestion d'identité et leurs terminaux d'envoi de données soient journalisées et assujetties à des politiques et à des procédures officielles de contrôle des changements.

**Surveillance et analyse des journaux**

1.13. Les DRS devraient mettre en place des processus automatiques de consolidation des journaux pour leurs services de gestion d'identité et leurs terminaux d'envoi de données vers des serveurs centralisés de gestion des journaux.

1.14. Les DRS devraient implanter des outils automatisés dans leurs systèmes d'information pour convertir les journaux des services de gestion d'identité et des terminaux d'envoi de données de contenus et de formats différents en un seul format standard avec des champs de données uniformes.

1.15. Les DRS devraient surveiller les journaux de leurs services de gestion d'identité et leurs terminaux d'envoi de données pour vérifier les points suivants :

1.15.1. les éléments qui déclenchent la création d'un journal sont bien configurés;

1.15.2. les éléments qui déclenchent la création d'un journal ne sont pas compromis;

1.15.3. les défectuosités sont repérées et font l'objet d'une analyse pour déterminer les correctifs nécessaires;

1.15.4. les défectuosités repérées sont résolues ou atténuées.

1.16. Les DRS doivent être en mesure de faire des corrélations entre les journaux de leurs services de gestion d'identité et de leurs terminaux d'envoi de données pour contribuer à la détection et à la prévention de l'usage impropre des renseignements et des systèmes d'information ou de toute intrusion.

1.17. Les DRS devraient implanter des outils qui font automatiquement des corrélations entre les activités inscrites dans les journaux de leurs services de gestion d'identité et de leurs terminaux d'envoi de données.

1.18. Les DRS devraient passer en revue les journaux de leurs services de gestion d'identité et de leurs terminaux d'envoi de données au moins une fois par mois.

1.19. Les DRS devraient veiller à ce que les journaux des administrateurs et des opérateurs de leurs services de gestion d'identité et de leurs terminaux d'envoi de données fassent l'objet d'un examen au moins une fois par trimestre.

1.20. La personne qui effectue l'examen des journaux des services de gestion d'identité et des terminaux d'envoi de données ne devrait pas être l'administrateur du système d'où proviennent les journaux.

**Conservation et entreposage des journaux**

1.21. Les DRS devraient veiller à ce que les journaux liés à leurs services de gestion d'identité et à leurs terminaux d'envoi de données soient facilement accessibles en ligne, au moins pour la durée indiquée dans la norme pour les fournisseurs d'identités fédérées et la politique de conservation des données du Comité ConnexionConfidentialité. Les journaux doivent être accessibles si on veut accélérer les enquêtes conformément à la norme.

1.22. Les DRS doivent conserver les journaux des services de gestion d'identité et des terminaux d'envoi de données pendant au moins la durée indiquée dans la norme pour les fournisseurs d'identités fédérées et la politique sur la conservation des données du Comité ConnexionConfidentialité, que le service soit assuré par le DRS, un mandataire ou un fournisseur de services électroniques.

1.23. Les DRS doivent archiver les journaux de leurs services de gestion d'identité et de leurs terminaux d'envoi de données dans un format qu'il est possible de restaurer aussi longtemps que les données doivent être conservées.

1.24. Les DRS devraient nommer et entreposer les journaux archivés de leurs services de gestion d'identité et de leurs terminaux d'envoi de données de manière organisée facilitant leur récupération.

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

2.1. L'équipe de [la solution de DSE] doit journaliser toutes les activités dans les systèmes d'information indiquées à l'annexe A intitulée *Sources et contenu des journaux* réalisées par les patients, un DRS, un mandataire et un fournisseur de services électroniques ayant accès à [la solution de DSE].

2.2. L'équipe de [la solution de DSE] doit veiller à ce que ses capacités de journalisation soient opérationnelles en tout temps. L'équipe de [la solution de DSE] doit configurer ses systèmes d'information de manière à qu'ils soient désactivés si la journalisation n'est pas opérationnelle.

2.3. L'équipe de [la solution de DSE] doit veiller à ce que tous les journaux soient classifiés selon le plus haut degré d'importance des renseignements qui s'y trouvent.

**Création de journaux**

2.4. L'équipe de [la solution de DSE] doit journaliser toutes les activités des administrateurs et opérateurs de ses systèmes d'information dans le cadre du processus de création du journal d'audit.

2.5. L'équipe de [la solution de DSE] doit veiller à ce que tous les journaux contiennent au moins les renseignements suivants pour chaque activité lorsque la situation s'y prête :

2.5.1. les identifiants (le plus possible d'entre eux) de l'entité qui demande l'action (nom d'utilisateur, nom de l'ordinateur, adresse IP et adresse MAC, par exemple);

2.5.2. les identifiants (le plus possible d'entre eux) de l'objet dans lequel a été accomplie l'action (nom des fichiers, identifiants uniques des registres consultés dans une base de données, adresse IP et adresse MAC, par exemple);

2.5.3. la date et l'heure;

2.5.4. l'activité comme telle (ouverture ou fermeture de session, par exemple);

2.5.5. l'état de l'activité (accès accordé ou refusé, par exemple);

2.5.6. le type d'accès (lecture seule, écriture, exécution);

2.5.7. les alertes envoyées par les systèmes de contrôle de l'accès et de surveillance du réseau.

2.6. L'équipe de [la solution de DSE] ne doit pas filtrer les journaux à la source.

2.7. L'équipe de [la solution de DSE] doit synchroniser les horloges de ses systèmes d'information avec une horloge centralisée. L'équipe de [la solution de DSE] doit valider la synchronisation des horloges au moins une fois par jour pour que les horloges indiquent toujours la même heure entre elles.

**Protection des journaux**

2.8. L'équipe de [la solution de DSE] doit implanter des mesures de contrôle visant à protéger la confidentialité et l'intégrité des journaux pendant leur entreposage et leur transmission.

2.9. L'équipe de [la solution de DSE] doit restreindre l'accès aux journaux selon les principes de privilège minimal et de besoin de savoir.

2.10. L'équipe de [la solution de DSE] doit conserver une liste de tous les mandataires et les fournisseurs de services électroniques qui ont l'autorisation d'accéder aux journaux. Cette liste doit contenir au minimum les éléments suivants :

2.10.1. le nom complet du mandataire ou du fournisseur de services électroniques;

2.10.2. le numéro de téléphone au travail du mandataire ou du fournisseur de services électroniques;

2.10.3. le courriel au travail du mandataire ou du fournisseur de services électroniques;

2.10.4. l'identifiant qu'a utilisé le mandataire ou le fournisseur de services électroniques pour l'accès logique au journal;

2.10.5. le nom du journal (ainsi que son type) auquel a accès le mandataire ou le fournisseur de services électroniques.

2.11. L'équipe de [la solution de DSE] ne doit pas configurer les journaux de telle manière que les anciennes données sont écrasées lorsque la limite de taille du journal est atteinte.

2.12. L'équipe de [la solution de DSE] doit interdire à ses mandataires et à ses fournisseurs de services électroniques ayant accès aux journaux de supprimer ou de désactiver les journaux de leurs propres activités.

2.13. L'équipe de [la solution de DSE] doit veiller à ce que les activités de gestion des sources de création de journaux soient journalisées et assujetties à des politiques et à des procédures officielles de contrôle des changements.

**Surveillance et analyse des journaux**

2.14. L'équipe de [la solution de DSE] devrait mettre en place des processus automatiques de consolidation des journaux pour ses systèmes d'information vers des serveurs centralisés de gestion des journaux.

2.15. L'équipe de [la solution de DSE] devrait implanter des outils automatisés dans ses systèmes d'information pour convertir les journaux de contenus et de formats différents en un seul format standard avec des champs de données uniformes.

2.16. L'équipe de [la solution de DSE] doit surveiller ses journaux pour vérifier les points suivants :

2.16.1. les éléments qui déclenchent la création d'un journal sont bien configurés;

2.16.2. les éléments qui déclenchent la création d'un journal ne sont pas compromis;

2.16.3. les défectuosités sont repérées et font l'objet d'une analyse pour déterminer les correctifs nécessaires;

2.16.4. les défectuosités repérées sont résolues ou atténuées.

2.17. L'équipe de [la solution de DSE] doit mettre en place des outils d'analyse automatique dans ses systèmes d'information pour contribuer à la détection et à la prévention de l'usage impropre des renseignements et des systèmes d'information ou de toute intrusion.

2.18. L'équipe de [la solution de DSE] doit implanter dans ses systèmes d'information des outils qui font automatiquement des corrélations entre les activités dans plusieurs systèmes d'information.

2.19. L'équipe de [la solution de DSE] doit veiller à ce que des alarmes automatiques aient lieu en cas de tentatives d'authentification échouées.

2.20. L'équipe de [la solution de DSE] doit passer en revue ses journaux au moins une fois par mois pour détecter les anomalies dans le réseau ou des comportements de mandataires ou de fournisseurs de services électroniques qui ne respectent pas la norme ou les procédures en vigueur ou voir d'où viennent les alertes indiquant une attaque ou une intrusion potentielle.

2.21. L'équipe de [la solution de DSE] doit veiller à ce que les journaux des administrateurs et des opérateurs de leurs systèmes d'information fassent l'objet d'un examen au moins une fois par mois.

2.22. L'équipe de [la solution de DSE] doit veiller à ce que la personne qui effectue l'examen des journaux des systèmes d'information ne devrait pas être l'administrateur du système d'où proviennent les journaux.

**Conservation et entreposage des journaux**

2.23. L'équipe de [la solution de DSE] doit veiller à ce que les journaux liés aux données de production soient facilement accessibles en ligne, pendant au moins six mois.

2.24. L'équipe de [la solution de DSE] doit conserver les journaux archivés des systèmes d'information au moins pour la durée indiquée dans la politique sur la conservation des données du Comité ConnexionConfidentialité.

2.25. L'équipe de [la solution de DSE] doit conserver les journaux archivés des activités des patients, des DRS, des mandataires et des fournisseurs de services électroniques conformément à la politique sur la conservation des données de [la solution de DSE].

2.26. L'équipe de [la solution de DSE] doit veiller à ce que les journaux liés aux sauvegardes soient facilement accessibles en ligne pour aussi longtemps que les journaux liés aux données de production.

2.27. L'équipe de [la solution de DSE] doit archiver ses journaux dans un format qu'il est possible de restaurer aussi longtemps que les données doivent être conservées.

2.28. L'équipe de [la solution de DSE] devrait nommer et entreposer ses journaux archivés de manière organisée facilitant leur récupération.

2.29. À l'expiration de la période de conservation, l'équipe de [la solution de DSE] doit veiller à ce que ses journaux soient supprimés conformément aux exigences de la Norme sur la gestion de l'information et des éléments d'actif.

**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 27001:2005 – Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences
- ISO/IEC 27002:2005 – Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information
- ISO/IEC 27005:2008 – Technologies de l'information – Techniques de sécurité – Gestion des risques en sécurité de l'information
- ISO 27799:2008 – Informatique de santé – Management de la sécurité de l'information relative à la santé en utilisant l'ISO/CEI 27002
- Publication spéciale du NIST 800-22, révision 1a – A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications
- FIPS 140-2 – Security Requirements for Cryptographic Modules

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

- Politique de sécurité de l'information
- Norme d'utilisation acceptable des données et des technologies de l'information
- Norme sur le contrôle de l'accès aux systèmes et les processus de gestion d'identité connexes
- Norme sur les pratiques d'inscription des autorités locales d'enregistrement (en anglais)
- Norme de Santé Ontario au sujet des prestataires qui assurent la gestion fédérée de l'identité (en anglais)
- Norme sur la cryptographie
- Norme sur les fournisseurs de services électroniques
- Norme sur la gestion des incidents de sécurité de l'information
- Norme sur la gestion de l'information et des éléments d'actif
- Norme sur les réseaux et les opérations
- Norme sur la journalisation de sécurité et la surveillance
- Norme sur le cycle de développement de systèmes
- Norme sur la sécurité matérielle
- Norme sur la gestion des menaces et des risquesPolitiques harmonisées sur la protection de la vie privée (en anglais)

**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 : Sources et contenu des journaux

| Système/logiciel | Activité à enregistrer |
|---|---|
| **Logiciel anti-programmes malveillants** *(comme les antivirus, les anti-espiogiciels et les détecteurs de programmes malveillants furtifs)* | • Cas de programmes malveillants détectés<br>• Tentatives de désinfection des fichiers et du système d'information<br>• Fichiers en quarantaine<br>• Recherches de programmes malveillants<br>• Mises à niveau de la signature ou du logiciel |
| **Systèmes de détection et de prévention des intrusions** | • Comportement suspicieux<br>• Attaques détectées<br>• Actions réalisées pour mettre fin à l'activité malveillante |
| **Systèmes d'accès à distance ou sans fil** | • Tentatives d'ouverture de session<br>• Quantité de données envoyées et reçues pendant la session |
| **Serveurs mandataires sur le Web** | • Adresses consultées |
| **Logiciel de gestion des vulnérabilités** *(comme les logiciels de gestion des correctifs et d'évaluation des vulnérabilités)* | • Historique d'installation des correctifs<br>• État de la vulnérabilité<br>• Vulnérabilités connues<br>• Mises à jour logicielles manquantes |
| **Serveurs d'authentification** *(comme les serveurs répertoires et les serveurs d'authentification unique)* | • Tentatives d'authentification |
| **Routeurs et commutateurs** | • Activité bloquée |
| **Pare-feu** | • Journaux détaillés de l'activité sur le réseau |
| **Serveurs de mises en quarantaine** | • État des vérifications de sécurité des hôtes<br>• Hôtes en quarantaine et raison |
| **Services de gestion d'identité** | • Consulter la section Création de journaux de la présente politique et la norme pour les fournisseurs d'identités fédérées |
| **Terminaux d'envoi de données** | • Consulter la section Création de journaux de la présente politique |
| **Systèmes d'exploitation** *(comme ceux des serveurs, des postes de travail et des appareils de connexion au réseau tels que les routeurs et les commutateurs)* | • Événements dans le système<br>  ○ Mise hors fonction du système<br>  ○ Démarrage des services<br>• Événements de sécurité<br>  ○ Accès à un fichier<br>  ○ Changements dans une politique<br>  ○ Changements dans un compte |

| | | |
|---|---|---|
| **Applications**<br>*(comme les serveurs et les clients de messagerie électronique, les serveurs Web, les fureteurs, les serveurs de fichiers et les clients de partage de fichiers et les serveurs de bases de données)*<br><br>** Nota : Consultez la politique harmonisée sur la journalisation et la vérification pour voir les exigences de journalisation et d'audit relatives aux applications (renseignements personnels sur la santé).* | • Demandes des clients et réponses des serveurs<br>• Tentatives d'authentification<br>• Changements dans un compte<br>• Recours à des privilèges<br>• Nombre de transactions et taille des transactions<br>• Événements de nature opérationnelle<br>  ○ Démarrage et mise hors fonction | • Changements de configuration<br>• Événements propres à l'application :<br>  ○ Envois et réceptions de courriels<br>  ○ Accès à un fichier<br>  ○ Demande de service<br>  ○ Transactions à l'échelle du système<br>  ○ Tâche accomplie (lecture, écriture, modification, suppression) |
| **Journaux des applications mobiles** | • Défaillances de validation de l'entrée/sortie des applications mobiles<br>• Réussites et échecs de l'authentification<br>• Échecs de l'autorisation (contrôle de l'accès); échecs de la gestion des sessions<br>• Utilisation de fonctionnalités à risque plus élevé (p. ex., connexions réseau non sécurisées, erreurs d'application et événements du système; acceptations légales et autres) | |