Ontario Health

Norme d’utilisation acceptable des données et des technologies de l’information

Version: 2.0

Identificateur de document : 3534

Avis de droit d'auteur

© Santé Ontario, 2021

Tous droits réservés

Il est interdit de reproduire le présent document, en totalité ou en partie, de quelque manière que ce soit, y compris en le photocopiant ou en le transférant en format électronique sur un ordinateur, sans d'abord obtenir une autorisation écrite de Santé Ontario. Les renseignements présentés dans le présent document sont la propriété de Santé Ontario, et il est interdit de les utiliser ou de les divulguer, sauf autorisation écrite expresse de Santé Ontario.

Marques de commerce

Les autres noms de produits mentionnés dans le présent document peuvent être des marques de commerce ou des marques de commerce déposées, et sont ici reconnus comme étant la propriété de leurs entreprises respectives.

Gestion du document

Date de la prochaine révision : Chaque année ou à la fréquence établie par le Comité ConnexionSécurité.

Historique des approbations

APPROBATEURS	DATE D'APPROBATION
Comité ConnexionSécurité	2017-02-21
Comité ConnexionSécurité	2018-03-26
Comité ConnexionSécurité	2019-07-04
Comité ConnexionSécurité	2021-03-18

Historique des modifications

NUMÉRO DE VERSION	DATE	RÉSUMÉ DES CHANGEMENTS	AUTEUR DES CHANGEMENTS
1.0	2013-11-18	Adoption de la version de novembre 2013 par le groupe de travail sur la protection de la vie privée et la sécurité de ConnexionRGT.	Mark Carter
1.1	2014-08-18	Mise à jour à partir des commentaires formulés par les membres du Comité ConnexionSécurité : ajout des notes de bas de page 1 et 2; réalignement du point 1.8 sous *Envoi de renseignements personnels sur la santé par courriel*; précision linguistique aux points 1.24 et 2.32; ajout des points 1.25 et 1.26; suppression du point 2.1; ajout de contexte au point 2.11; alignement des références.	Mark Carter
1.2	2014-10-09	Examen à partir des commentaires du Comité ConnexionSécurité reçus le 9 septembre 2014 : remplacement de « nom d'utilisateur et mot de passe » par « données d'identification » aux points 1.1 et 1.2; ajout de « contourner en toute connaissance de cause » au point 1.4 pour accroître la portée de l'énoncé; au point 1.8, ajout d'une exigence de verrouillage des ordinateurs laissés sans surveillance pour tous les utilisateurs; aux points 1.9 et 2.5, changer « appareils » pour « outils et processus »; aux points 1.13 et 2.19, ajout d'une nuance sous la forme du libellé « dans la mesure du possible »; au point 1.21, ajout d'un énoncé sur le signalement des incidents; au point 1.22, ajout de la possibilité d'approbation de l'identification unique par les gestionnaires; au point 1.23, ajout d'une référence sur la norme en matière de nom d'utilisateur et de mot de passe; au point 1.30, exigence de chiffrement intégral du disque dur sur lequel sont stockées	Mark Carter

NUMÉRO DE VERSION	DATE	RÉSUMÉ DES CHANGEMENTS	AUTEUR DES CHANGEMENTS
		les données et pour les utilisations à distance.	
1.3	2014-10-16	Révision à la suite de la réunion du Comité ConnexionSécurité du 15 octobre. Mise à jour du point 1.30 afin d'y inclure les implantations acceptables de chiffrement sur les appareils.	Mark Carter
1.4	2014-11-05	Révision à la suite de la réunion du Comité ConnexionSécurité du 5 novembre. Changement du verbe au point 1.8 pour « doit »; reformulation du point 1.10; et au point 1.30, mention de la méthode privilégiée de chiffrement intégral du disque dur. Le Comité ConnexionSécurité a approuvé la politique.	Mark Carter
1.5	2015-01-21	Harmonisation des libellés à la *Politique de contrôle des accès et de gestion de l'identité* (en anglais) conformément à la décision définitive de la 3e étape du Comité ConnexionSécurité.	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	2017-02-21	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
1.8	16 mars 2018	Mise à jour de la norme afin d'inclure l'accès du patient au DSE et les recommandations du NIST relatives aux mots de passe (NIST 800-63B).	Geovanny Diaz / Ola Edidi
1.9	4 juillet 2019	Mise à jour de la norme afin d'exiger le verrouillage des appareils et l'utilisation de phrases de passe.	Ravi Addepalli
2.0	2021-01-04	Examen du document avec des modifications mineures, mise à jour du modèle et du cycle de revision tous les deux ans	Ana Fukushima

Utilisation acceptable des données et des technologies de l'information

Objectif

La présente norme vise à définir les exigences en matière d'utilisation pour les mandataires et les fournisseurs de services électroniques de [la solution de DSE], ainsi que les dépositaires de renseignements sur la santé, leurs mandataires et leurs fournisseurs de services électroniques ayant accès à [la solution de DSE]. Ces exigences ont pour objectif de protéger la confidentialité, l'intégrité et la disponibilité des renseignements personnels sur la santé stockés ou traités dans [la solution de DSE].

Portée

La présente norme s'applique :

- aux mandataires et aux fournisseurs de services électroniques de [la solution de DSE], y compris la totalité des portails et des applications pour les patients;

- aux dépositaires de renseignements sur la santé, à leurs mandataires et à leurs fournisseurs de services électroniques ayant l'autorité de création, de contribution, de visualisation et d'accès à [la solution de DSE].

La présente norme ne s'applique pas :

- aux dépositaires de renseignements sur la santé, à leurs mandataires ou à leurs fournisseurs de services électroniques n'ayant pas autorité de création, de contribution, de visualisation ou d'accès à [la solution de DSE].

Définitions

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

[la solution de DSE] : [la solution de DSE] et les systèmes de soutien destinés au stockage et à la consultation par voie électronique de certains renseignements personnels sur la santé provenant des systèmes 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.

Fournisseur de services électroniques : Une personne qui fournit des biens ou des services en vue de permettre à un dépositaire de renseignements sur la santé, par voie électronique, de recueillir, d'utiliser, de modifier, de divulguer, de conserver ou d'éliminer des renseignements personnels sur la santé, notamment le fournisseur d'un réseau d'information sur la santé.

Technologie de l'information : Tout bien (matériel ou logique) servant à l'acquisition, au stockage, à la manipulation, à la gestion, au transfert, au contrôle, à l'affichage, à la commutation, à l'échange, à la transmission ou à la réception automatiques de données ou de renseignements. Il peut s'agir par exemple de matériel, de logiciels, de micrologiciels, d'équipement auxiliaire, ou de ressources connexes.

Doit/doivent : Ces termes indiquent des exigences non facultatives.

Préférable ou devrait/devraient : Ces termes sont employés lorsque les utilisateurs, dans certains cas, peuvent avoir des raisons valables de ne pas respecter l'exigence. Toutefois, le responsable de la mise en œuvre doit être conscient des conséquences de ce geste et envisager d'instaurer des mesures de contrôle compensatoires.

Peut/peuvent : L'exigence n'est en fait qu'une recommandation, ou une liste d'exemples qui ne se veut pas exhaustive.

Exigences de la norme

1. Exigences visant les dépositaires de renseignements sur la santé, leurs mandataires et leurs fournisseurs de services électroniques

Les dépositaires de renseignements sur la santé, leurs mandataires et leurs fournisseurs de services électroniques (« tous les utilisateurs ») doivent respecter les exigences suivantes :

1.1. Toujours se servir des données d'identification qui leur ont été assignées pour participer à [la solution de DSE].

1.2. Ne jamais laisser une autre personne se servir de leurs données d'identification pour participer à [la solution de DSE]. Tous les utilisateurs sont responsables des actions exécutées sur [la solution de DSE] à l'aide de leur nom d'utilisateur.

1.3. Participer à [la solution de DSE] uniquement si leurs fonctions l'exigent, s'ils y sont expressément autorisés, s'il est nécessaire de le faire (p. ex., pour fournir des soins de santé ou faciliter leur prestation), et conformément aux politiques de confidentialité liées à [la solution de DSE] ou celles de leurs dépositaires de renseignements sur la santé respectifs.

1.4. Ne jamais désactiver, outrepasser ou contourner en toute connaissance de cause les mesures de contrôle de la sécurité de l'information lors de la participation à [la solution de DSE].

1.5. Ne jamais tenter d'exploiter des failles de sécurité potentielles, même pour vérifier si elles existent vraiment, à moins que cela ne fasse partie des tâches et responsabilités qui leur sont assignées dans le cadre de leur travail et que les responsables de [la solution de DSE] les y aient expressément autorisés.

1.6. Ne jamais réaliser sciemment une action qui nuira au fonctionnement normal de [la solution de DSE], ou tenter de perturber la solution en la rendant intentionnellement indisponible ou en portant atteinte à l'intégrité des données qui y sont stockées ou traitées pour la participation à la [solution de DSE].

1.7. Respecter les modalités d'utilisation de [la solution de DSE].

1.8. Dans les installations des dépositaires de renseignements sur la santé, tous les utilisateurs doivent verrouiller leur appareil informatique quand ils le laissent sans surveillance et qu'une session de [la solution de DSE] y est ouverte.

1.9. Utiliser les outils et les processus de [la solution de DSE] ou ceux utilisés par le dépositaire de renseignements sur la santé pour participer à la solution.

1.10. Ne jamais prendre en photo des données affichées dans [la solution de DSE].

Envoi de renseignements personnels sur la santé par courriel[1]

Tous les utilisateurs doivent respecter les exigences suivantes :

1.11. Envoyer des renseignements personnels sur la santé aux responsables de [la solution de DSE] par courriel uniquement si c'est nécessaire pour offrir des soins de santé ou faciliter leur prestation ou dans le cadre du fonctionnement de [la solution de DSE], et si c'est acceptable selon les politiques ou procédures relatives à [la solution de DSE] ou celles de leurs dépositaires de renseignements sur la santé respectifs.

1.12. Chiffrer les courriels contenant des renseignements personnels sur la santé, utiliser une solution de transfert de fichiers sécuritaire ou se servir d'un système de courriel sécuritaire et approuvé par leurs dépositaires de renseignements sur la santé respectifs ou [la solution de DSE].

1.13. Ne jamais envoyer de renseignements personnels sur la santé provenant de [la solution de DSE] à l'aide de comptes de courriel externes (p. ex., Hotmail ou Gmail), ou les faire envoyer à ce type de comptes.

Création et protection de mots de passe[2]

Tous les utilisateurs doivent respecter les exigences suivantes :

1.14. Utiliser des phrases (p. ex., « Ja1meLaP!zza ») comme mots de passe pour participer à [la solution de DSE].

Tous les utilisateurs doivent respecter les exigences suivantes :

1.15. Pour participer à la [solution de DSE], toujours créer des mots de passe composés de huit caractères minimum, avec un maximum de 64 caractères, satisfaisant au moins trois des conditions de complexité suivantes :

1.15.1. Un chiffre;

1.15.2. Une lettre majuscule;

1.15.3. Une lettre minuscule;

1.15.4. Un caractère spécial.

[1] Cette section ne s'applique qu'aux mots de passe permettant d'accéder directement à la [solution de DSE]. Elle ne vise pas les pratiques d'envoi de courriel à l'interne des dépositaires de renseignements sur la santé.
[2] Cette section ne s'applique qu'aux mots de passe permettant d'accéder directement à la [solution de DSE].

Pour permettre l'absence de complexité, la vérification en direct des nouveaux mots de passe doit être effectuée et présentée aux utilisateurs pendant la création des mots de passe. La vérification en direct doit effectuer une comparaison avec une liste de mots de passe couramment utilisés : liste noire, dictionnaire, noms d'utilisateurs, noms de services, chaînes séquentielles et mots de passe utilisés lors de brèches précédentes.

1.16. Ne jamais créer de mots de passe utilisés pour participer à la [solution de DSE] qui comportent :

1.16.1. Une partie ou la totalité de leur nom d'utilisateur;

1.16.2. Des renseignements personnels faciles à obtenir (p. ex., nom de membres de la famille ou d'animaux de compagnie, dates de naissance, anniversaires, ou passe-temps);

1.16.3. Trois caractères consécutifs (p. ex., AAA).

1.17. Pour participer à la [solution de DSE], choisir des mots de passe facilement mémorisables, mais difficiles à deviner par d'autres personnes.

1.18. Ne jamais modifier de manière facilement prévisible les mots de passe utilisés pour participer à la [solution DES] (p. ex., changer « Ja1meLaP!zza1 » pour « Ja1meLaP!zza2 »).

1.19. Pour participer à la [solution DES], employer des mots de passe différents de ceux d'autres comptes (p. ex., compte de messagerie courriel de l'établissement ou compte bancaire personnel).

1.20. Mémoriser les mots de passe servant à participer à [la solution de DSE]. Les utilisateurs doivent éviter de tenir un registre de leurs mots de passe (p. ex., les inscrire sur une feuille ou dans un fichier), sauf :

1.20.1. Si ceux-ci peuvent être stockés de manière sécuritaire;

1.20.2. Si le nom d'utilisateur n'est pas indiqué ou s'il s'agit du mot de passe de [la solution de DSE].

1.21. Garder secrets les mots de passe permettant de participer à [la solution de DSE] et ne jamais les révéler à quiconque, pas même à un administrateur du système, à un employé d'un service de dépannage ou à un gestionnaire.

1.22. Changer immédiatement le mot de passe servant à participer à [la solution de DSE] s'ils soupçonnent ou découvrent que celui-ci a été divulgué ou compromis, et signaler l'incident lié à la sécurité de l'information au premier point de contact responsable (p. ex., service de dépannage ou responsable de la protection de la vie privée). Voir la section Signalement des incidents liés à la sécurité de l'information de [la solution de DSE] ci-après.

1.23. Ne pas intégrer le nom d'utilisateur ou le mot de passe permettant de participer à [la solution de DSE] dans un processus d'identification unique (p. ex., macro-instruction ou touche de gestion programmable), sauf pour les systèmes de gestion de l'identification approuvés pour [la solution de DSE].

1.24. Toujours modifier le mot de passe initial fourni pour la première connexion à [la solution de DSE] et conformément aux directives du fournisseur de données d'identification.

Travail à distance

Tous les utilisateurs doivent respecter les exigences suivantes :

1.25. Utiliser une solution d'accès à distance approuvée par [la solution de DSE] ou les dépositaires de renseignements sur la santé (p. ex., réseau privé virtuel ou terminal) pour participer à distance à [la solution de DSE].

1.26. Suivre la procédure de déconnexion adéquate lors d'un accès à distance utilisé pour participer à [la solution de DSE] (p. ex., si la solution d'accès à distance dispose d'une fonction de déconnexion, utiliser cette dernière au lieu de simplement fermer l'application).

1.27. Ne jamais participer à [la solution de DSE] dans un lieu où des personnes non autorisées peuvent voir les renseignements affichés à l'écran (p. ex., cafés Internet, transports publics et autres lieux publics).

1.28. Ne jamais laisser un appareil informatique mobile pouvant participer à [la solution de DSE] sans surveillance dans un endroit public.

1.29. Lorsqu'il est nécessaire de laisser un appareil informatique mobile dans un véhicule, tous les utilisateurs doivent le placer hors de vue et verrouiller le véhicule.

1.30. Si des renseignements sur la santé ou des renseignements personnels de [la solution de DSE] sont sauvegardés sur un appareil informatique sans fil, s'assurer que le disque sur lesquels sont sauvegardés les données est doté d'un système de chiffrement intégral ou que le système de l'utilisateur effectue un chiffrement intégral du disque. Le chiffrement intégral du disque de l'appareil informatique sans fil est la méthode privilégiée; toutefois, l'implantation du chiffrement conteneurisé du disque partagé et de l'appareil d'entreprise est aussi acceptable.

Signalement des incidents liés à la sécurité de l'information de [la solution de DSE]

Tous les utilisateurs doivent respecter les exigences suivantes :

1.31. Signaler immédiatement les incidents présumés ou constatés relativement à la sécurité de l'information de [la solution de DSE] au premier point de contact responsable (p. ex., service de dépannage ou responsable de la protection de la vie privée). Sinon, le dépositaire de renseignements sur la santé peut demander aux mandataires de signaler l'incident à leur gestionnaire ou superviseur, lequel avisera ensuite le premier point de contact.

Voici des exemples d'incidents liés à la sécurité de l'information :

- Divulgation non autorisée de renseignements personnels sur la santé;
- Vol ou perte de technologies de l'information contenant des renseignements personnels sur la santé ou ayant accès à [la solution de DSE] (même si elles sont chiffrées);
- Contamination par virus ou logiciel malveillant d'un appareil qui a accès à [la solution de DSE];
- Tentatives (réussies ou ratées) d'accès non autorisé à [la solution de DSE];

- Mot de passe compromis (c'est-à-dire qu'une autre personne connaît votre mot de passe permettant d'accéder à [la solution de DSE]).

1.32. Offrir leur entière collaboration aux responsables de [la solution de DSE], à ses mandataires ou à ses fournisseurs de services électroniques dans le cadre de toute enquête sur des incidents liés à la sécurité de l'information.

2. Mandataires et fournisseurs de services électroniques de [la solution de DSE]

Les mandataires et les fournisseurs de services électroniques de [la solution de DSE] (« tous les utilisateurs ») doivent respecter les exigences suivantes :

2.1. Toujours se servir du nom d'utilisateur et du mot de passe qui leur ont été assignés pour participer à [la solution de DSE].

2.2. Ne jamais laisser une autre personne se servir de leur nom d'utilisateur pour participer à [la solution de DSE]. Tous les utilisateurs sont responsables des actions exécutées sur [la solution de DSE] l'aide de leur nom d'utilisateur.

2.3. Participer à [la solution de DSE] uniquement si leurs fonctions l'exigent, s'ils y sont expressément autorisés, s'il est nécessaire de le faire (p. ex., pour fournir des soins de santé ou faciliter leur prestation), et conformément aux politiques de confidentialité liées à [la solution de DSE].

2.4. Ne jamais désactiver ou outrepasser les mesures de contrôle de la sécurité de l'information (p. ex., désactiver le logiciel antivirus de leur poste de travail).

2.5. Utiliser exclusivement les outils et processus autorisés ou recommandés pour [la solution de DSE] afin de participer à la solution.

2.6. Ne jamais tenter d'exploiter des failles de sécurité potentielles, même pour vérifier si elles existent vraiment, à moins que cela ne fasse partie des tâches et responsabilités qui leur sont assignées dans le cadre de leur travail et que les responsables de [la solution de DSE] les y aient expressément autorisés.

2.7. Ne jamais réaliser sciemment une action qui nuira au fonctionnement normal de [la solution de DSE], ou tenter de perturber la solution en la rendant intentionnellement indisponible ou en portant atteinte à l'intégrité des données qui y sont stockées ou traitées.

2.8. Respecter les modalités d'utilisation de [la solution de DSE].

Protection des renseignements personnels sur la santé

Tous les utilisateurs doivent respecter les exigences suivantes :

2.9. Ne jamais discuter de renseignements personnels sur la santé avec une personne n'ayant pas besoin de savoir ou qui n'est pas autorisée à connaître ces renseignements.

2.10. Ne jamais discuter de renseignements personnels sur la santé dans des aires publiques, comme les ascenseurs, car la conversation pourrait facilement être entendue par des personnes n'ayant pas besoin de savoir.

2.11. Garder les renseignements personnels sur la santé sous clé (p. ex., en plaçant dans une armoire fermée à clé les données de [la solution de DSE] qui sont imprimées ou sauvegardées sur un support amovible) lorsqu'ils sont laissés sans surveillance dans une aire non sécurisée, en particulier lorsque personne n'est présent dans le bureau ou l'aire en question.

2.12. Toujours fermer ou verrouiller la session des ordinateurs ou postes de travail laissés sans surveillance pour empêcher des personnes non autorisées de consulter les renseignements personnels sur la santé.

2.13. Stocker les renseignements personnels sur la santé uniquement sur des appareils ou réseaux de stockage approuvés par [la solution de DSE], et ne stocker que les renseignements nécessaires sur les supports de stockage amovibles chiffrés.

2.14. Toujours déchiqueter les documents papier contenant des renseignements personnels sur la santé ou les placer dans des boîtes sécurisées pour le déchiquetage lorsqu'ils ne sont plus requis.

2.15. Respecter la procédure interne d'élimination adéquate et sécuritaire des technologies de l'information pouvant contenir des renseignements personnels sur la santé.

Envoi de renseignements personnels sur la santé par courriel

Tous les utilisateurs doivent respecter les exigences suivantes :

2.16. Envoyer des renseignements personnels sur la santé par courriel uniquement si c'est nécessaire pour offrir des soins de santé ou faciliter leur prestation ou dans le cadre du fonctionnement de [la solution de DSE], et si c'est acceptable selon les politiques ou procédures relatives à [la solution de DSE].

2.17. Chiffrer les courriels contenant des renseignements personnels sur la santé, utiliser une solution de transfert de fichiers sécuritaire ou se servir d'un système de courriel sécuritaire et approuvé par [la solution de DSE].

2.18. Ne jamais envoyer de renseignements personnels à l'aide de comptes de courriel externes (p. ex., Hotmail ou Gmail), ou les faire envoyer à ce type de comptes.

Création et protection de mots de passe

Tous les utilisateurs devraient respecter les exigences suivantes :

2.19. Dans la mesure du possible, utiliser des phrases (p. ex., « Ja1meLaP!zza ») comme mots de passe.

Tous les utilisateurs doivent respecter les exigences suivantes :

2.20. Pour participer à la [solution de DSE], toujours créer des mots de passe composés de huit caractères minimum, avec un maximum de 64 caractères, satisfaisant au moins trois des conditions de complexité suivantes :

2.20.1. Un chiffre;

2.20.2. Une lettre majuscule;

2.20.3. Une lettre minuscule;

2.20.4. Un caractère spécial.

Pour permettre l'absence de complexité, la vérification en direct des nouveaux mots de passe doit être effectuée et présentée aux utilisateurs pendant la création des mots de passe. La vérification en direct doit effectuer une comparaison avec une liste de mots de passe couramment utilisés : liste noire, dictionnaire, noms d'utilisateurs, noms de services, chaînes séquentielles et mots de passe utilisés lors de brèches précédentes.

2.21. Ne jamais créer de mots de passe qui comportent :

2.21.1. Une partie ou la totalité de leur nom d'utilisateur;

2.21.2. Des renseignements personnels faciles à obtenir (p. ex., nom de membres de la famille ou d'animaux de compagnie, dates de naissance, anniversaires, passe-temps);

2.21.3. Trois caractères consécutifs (p. ex., AAA).

2.22. Choisir des mots de passe facilement mémorisables, mais difficiles à deviner par d'autres personnes.

2.23. Ne jamais modifier les mots de passe de manière facilement prévisible (p. ex., changer « Ja1meLaP!zza1 » pour « Ja1meLaP!zza2 »).

2.24. Pour participer à la [solution DSE], employer des mots de passe différents de ceux d'autres comptes (p. ex., compte de courriel de l'établissement, compte bancaire personnel, etc.).

2.25. Mémoriser les mots de passe. Les utilisateurs doivent éviter de tenir un registre de leurs mots de passe (p. ex., les inscrire sur une feuille ou dans un fichier), sauf :

2.25.1. Si ceux-ci peuvent être stockés de manière sécuritaire;

2.25.2. Si le nom d'utilisateur n'est pas indiqué, ou si le système d'information ou la technologie de l'information n'est pas précisé.

2.26. Garder les mots de passe secrets et ne jamais les révéler à quiconque, pas même à un administrateur du système, à un employé d'un service de dépannage ou à un gestionnaire.

2.27. Changer immédiatement le mot de passe s'ils soupçonnent ou découvrent que celui-ci a été divulgué ou compromis.

2.28. Ne pas intégrer le nom d'utilisateur ou le mot de passe dans un processus d'identification unique (p. ex., macro-instruction ou touche de gestion programmable).

2.29. Toujours modifier le mot de passe initial fourni pour la première connexion.

Travail à distance

Tous les utilisateurs doivent respecter les exigences suivantes :

2.30. Utiliser une solution de connexion d'accès à distance approuvée par [la solution de DSE] (p. ex., réseau privé virtuel ou terminal) pour participer à [la solution de DSE].

2.31. Suivre la procédure de déconnexion adéquate lors d'un accès à distance (p. ex., si la solution d'accès à distance dispose d'une fonction de déconnexion, utiliser cette dernière au lieu de simplement fermer l'application).

2.32. Ne jamais accéder à [la solution de DSE] dans un lieu où des personnes non autorisées peuvent voir les renseignements affichés à l'écran (p. ex., cafés Internet, transports publics et autres lieux publics).

2.33. Ne jamais laisser un appareil informatique mobile pouvant se connecter à [la solution de DSE] sans surveillance dans un endroit public.

2.34. Lorsqu'il est nécessaire de laisser un appareil informatique mobile dans un véhicule, toutes les personnes doivent le placer hors de vue et verrouiller le véhicule.

Signalement des incidents liés à la sécurité de l'information

Tous les utilisateurs doivent respecter les exigences suivantes :

2.35. Signaler immédiatement les incidents présumés ou constatés relativement à la sécurité de l'information au premier point de contact responsable de [la solution de DSE] (p. ex., un service de dépannage). Sinon, les mandataires peuvent signaler l'incident à leur gestionnaire ou superviseur, lequel avisera ensuite le premier point de contact.

Voici des exemples d'incidents liés à la sécurité de l'information :

- Divulgation non autorisée de renseignements personnels sur la santé;
- Vol ou perte de technologies de l'information contenant des renseignements personnels sur la santé (même si elles sont chiffrées);
- Contamination par virus ou logiciel malveillant d'un appareil qui a accès à [la solution de DSE];
- Tentatives (réussies ou ratées) d'accès non autorisé à [la solution de DSE];
- Mot de passe compromis (c'est-à-dire qu'une autre personne connaît votre mot de passe).

2.36. Offrir leur entière collaboration aux responsables de [la solution de DSE], à ses mandataires ou à ses fournisseurs de services électroniques dans le cadre de toute enquête sur des incidents liés à la sécurité de l'information.

Dérogation

Toute dérogation à la présente norme doit être approuvée par l'organisme de surveillance compétent, qui l'autorisera seulement si elle est clairement justifiée et n'a que la portée nécessaire pour satisfaire le besoin.

Voir l'*Annexe A : Demandes de dérogation aux exigences en matière de sécurité de l'information* de la *Politique de sécurité de l'information.*

Application

Tous les cas de non-conformité doivent être examinés par l'organisme de surveillance compétent.

L'organisme de surveillance compétent a le pouvoir d'imposer des sanctions, allant jusqu'à la révocation du privilège d'accès des mandataires ou des accords conclus avec les dépositaires de renseignements sur la santé et les fournisseurs de services électroniques, ainsi que des mesures correctives.

Référence

Loi et règlement

- *Loi de 2004 sur la protection des renseignements personnels sur la santé* (LPRPS), art. 12 et 13 et Partie V
- Règlement de l'Ontario 329/04, art. 6

Normes internationales

- ISO/CEI 27001 : 2005, Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences
- ISO/CEI 27002 : 2005, Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information
- ISO/CEI 27005 : 2008, Technologies de l'information – Techniques de sécurité – Gestion des risques liés à la 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

Documents liés au dossier de santé électronique 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 fournisseurs d'identités fédérées et Manuel de procédures relatives à l'admissibilité*
- *Norme sur la continuité des activités*
- *Norme sur la cryptographie*

- *Norme sur les fournisseurs de services électroniques*
- *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 risques*
- *Harmonized Privacy Protection Policies* (en anglais)

Inforoute Santé du Canada

- Inforoute Santé du Canada, Dossier de santé électronique (DSE) – *Exigences en matière de protection de la confidentialité et de sécurité* (version 1.1, révisée le 7 février 2005)

Autre référence

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