 Ministère de la Santé Gouvernement du Nunavut	DIRECTIVE DU MINISTÈRE DE LA SANTÉ		
	DIRECTIVE SUR LA SÉCURITÉ ET LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS LES DSEI		
TITRE :		SECTION :	NUMÉRO DE POLITIQUE :
Surveillance et audit de la mise en œuvre de la directive sur les systèmes de cybersanté			
DATE D'ENTRÉE EN VIGUEUR :	DATE DE RÉVISION :	REMPLECE LE NUMÉRO :	NOMBRE DE PAGES :
			4
APPLICABLE À :			
Tous les employés, fournisseurs et agents du GN qui utilisent les systèmes de cybersanté.			

1. PRÉAMBULE

La présente directive a pour but de guider les employés, fournisseurs et agents du gouvernement du Nunavut (GN) quant à la surveillance et à l'audit des utilisateurs et agents externes qui accèdent aux systèmes de cybersanté.

Le ministère de la Santé est assujéti à la Loi sur l'accès à l'information et à la protection de la vie privée (AIPVP), une loi qui a été édictée pour rendre les organismes publics redevables à la population par rapport au traitement des informations et à la protection de la vie privée. Les renseignements personnels sur la santé sont compris dans la définition des renseignements personnels de l'AIPVP.

L'article 42 de l'AIPVP requiert que le ministère de la Santé protège les renseignements personnels « en prenant les mesures de sécurité voulues contre des risques tels que l'accès, la collecte, l'usage, la divulgation et le retrait non autorisés. »

Les clients font confiance au GN et s'attendent à ce que celui-ci protège la confidentialité, l'intégrité et le caractère privé de leurs renseignements personnels. Il est essentiel de satisfaire ces attentes afin de promouvoir la sécurité des clients et gagner leur confiance et leur loyauté.

2. PRINCIPES

1. Le ministère de la Santé surveille et audite les accès aux systèmes de cybersanté conformément aux principes suivants :
 - a. la priorité de consolider les services publics en développant les infrastructures en cybersanté qui améliorent et rendent plus efficace et efficace la gestion des renseignements personnels;
 - b. l'*Inuit Qaujimagatuqangit* qui consiste en *Piliriqatigiinniq* (travailler ensemble vers un but commun), *Inuuqatigiitsiarniq* (respecter les autres, les relations et prendre soin des gens), *Tunnganarniq* (nourrir une bonne attitude en étant ouvert, accueillant et inclusif) et *Pilimmaksarniq* (acquérir des compétences par la pratique, l'effort et l'action);

- c. le GN, incluant le ministère de la Santé, a l'obligation légale de protéger les renseignements et dossiers personnels qu'il détient en prenant les mesures de sécurité voulues contre les risques tels l'accès, la collecte, l'usage, la divulgation et le retrait non autorisés de tels renseignements;
- d. les systèmes de cybersanté ne peuvent être accédés qu'à des fins autorisées seulement;
- e. le GN a le droit et le devoir de surveiller et d'auditer les accès des utilisateurs aux systèmes de cybersanté pour s'assurer que les renseignements personnels sont recueillis, utilisés et divulgués à des fins autorisées seulement;
- f. le GN a la responsabilité de protéger la confidentialité, l'intégrité et la disponibilité des renseignements personnels et autres ressources des systèmes de cybersanté.

3. PORTÉE ET APPLICATION

La présente directive ayant trait à la surveillance et l'audit des systèmes de cybersanté s'applique à :

- 1. tous les utilisateurs, incluant les employés, contractuels et agents du GN, ainsi que tous les vendeurs et fournisseurs de produits et services au GN qui accèdent aux systèmes de cybersanté, les utilisent, les opèrent ou les entretiennent.
- 2. tous les systèmes de cybersanté et aux ressources des systèmes connexes, incluant :
 - a. les données confidentielles :
 - i. renseignements personnels;
 - ii. journaux d'audit des systèmes;
 - iii. données administratives du système et de la sécurité (par ex. configurations de la sécurité technique, informations de mots de passe et d'authentification);
 - b. le matériel comme les appareils mobiles et l'équipement de réseautique;
 - c. les logiciels;
 - d. les ressources en communication et réseautique.

3. RÔLES ET RESPONSABILITÉS

- 1. La Division des renseignements sur la santé de la population (DRSP) a la responsabilité de surveiller et d'auditer les accès des utilisateurs aux renseignements personnels dans les systèmes de cybersanté.
- 2. L'agent de sécurité du ministère des Services communautaires et gouvernementaux (SCG) a la responsabilité de surveiller et d'auditer les systèmes de cybersanté pour savoir et intervenir lorsqu'il y a un accès non autorisé par un agent externe (par ex. un pirate informatique) qui menace la confidentialité, l'intégrité et la disponibilité des renseignements personnels et des ressources des systèmes de cybersanté.

4. JOURNAUX D'AUDIT

1. La DRSP et les SCG mettront en service une fonctionnalité permettant la production de journaux d'audit dans tous les systèmes de cybersanté.
2. La DRSP et les SCG définiront les paramètres des rapports d'audit devant être émis par les systèmes de cybersanté en fonction du risque qu'il y ait consultation, collecte, usage ou divulgation non autorisés de renseignements personnels ou de la menace à l'égard de la confidentialité, l'intégrité et la disponibilité des ressources des systèmes de cybersanté déterminée par l'évaluation des menaces et des risques (EMR).

5. PROGRAMME DE SURVEILLANCE ET D'AUDIT – ACCÈS DES UTILISATEURS

1. La DRSP établira un programme d'audit des accès des utilisateurs aux systèmes de cybersanté afin de s'assurer que ces systèmes et les renseignements personnels sont utilisés d'une manière appropriée par les utilisateurs autorisés.
2. La DRSP établira des critères pour l'identification des atteintes potentielles à la sécurité et à la vie privée en se basant sur les menaces relevées dans une évaluation des **répercussions sur la vie privée (ERVP)** ou une ÉMR, ou celles détectées dans le cadre de la mise en œuvre continue du programme. Ces critères peuvent inclure, sans toutefois s'y limiter, la consultation de dossiers médicaux :
 - a. de VIP ou de proches des employés du ministère de la Santé;
 - b. contenant des renseignements personnels relatifs à des maladies contagieuses, des infections sexuellement transmissibles, des résultats de tests de dépistage du VIH-Sida, la toxicomanie, la santé mentale ou d'autres informations hautement confidentielles;
 - c. depuis la résidence ou d'autres lieux éloignés;
 - d. à des heures inhabituelles (par ex. au milieu de la nuit).
3. Si un utilisateur est soupçonné d'avoir accédé à des renseignements personnels à des fins non reliées à son rôle ou à sa fonction professionnelle, la DRSP alertera le coordonnateur de l'AIPVP au ministère de la Santé.
4. Le coordonnateur de l'AIPVP effectuera une enquête et pourra exiger que la DRSP réalise un audit de tous les accès par l'utilisateur aux renseignements personnels et aux systèmes de cybersanté afin de déterminer s'il y a eu violation ou non en vertu de l'AIPVP et de la politique en matière d'atteinte à la vie **privée** (*Privacy Breach and Incident Policy*).
5. Le coordonnateur de l'AIPVP enquêtera sur tous les cas où il y a soupçon de violation de la vie privée.
6. Lorsqu'il est déterminé qu'il y a eu violation possible de la vie privée, le coordonnateur de l'AIPVP lance le protocole d'intervention en cas de violation de la vie privée prévu dans l'AIPVP et la politique en matière d'atteinte à la vie privée.

Comment [MD1]: À remplacer par le nom véritable de l'évaluation en français le cas échéant.

Comment [MD2]: Remplacer le titre traduit par le titre français le cas échéant.

6. PROGRAMME DE SURVEILLANCE ET D'AUDIT – AGENTS EXTERNES

1. Les SCG établiront un programme pour surveiller et auditer tous les accès non autorisés aux systèmes de cybersanté par des agents qui sont extérieurs aux infrastructures du GN.

2. Les SCG définiront des critères servant à identifier les atteintes potentielles à la sécurité en se basant sur les menaces relevées dans une ÉMR ou détectées dans le cadre de la mise en œuvre continue du programme.
3. Les SCG enquêteront sur tous les cas où il y a soupçon d'atteinte à la sécurité selon les critères définis.
4. Lorsque les SCG auront déterminé qu'il y a eu atteinte possible à la sécurité, ils en aviseront le coordonnateur de l'AIPVP qui lancera le protocole d'intervention en cas de violation de la vie privée prévu dans l'AIPVP et la politique en matière d'atteinte à la vie privée.

7. ADMINISTRATION DE LA PRÉSENTE DIRECTIVE

La présente directive est revue chaque année par les sous-ministres de la Santé et des Services communautaires et gouvernementaux ou dès qu'une enquête est déclenchée sur une présumée violation de la sécurité ou de la vie privée reliée à la surveillance ou à l'audit des systèmes de sécurité, ou encore lorsque l'évaluation des menaces et des risques ou l'audit de sécurité mène à des résultats négatifs. Le rapport de révision est remis aux ministres de la Santé et des Services communautaires et gouvernementaux.


8. AUTORISATION

Sous-ministre
Ministère de la Santé

Date

Sous-ministre
Ministère des Services communautaires
et gouvernementaux

Date

 Ministère de la Santé Gouvernement du Nunavut	DIRECTIVE DU MINISTÈRE DE LA SANTÉ		
	DIRECTIVE SUR LA SÉCURITÉ ET LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS LES DSEi		
TITRE :		SECTION :	NUMÉRO DE POLITIQUE :
Directive relative à la sécurité des informations dans les systèmes de cybersanté.			
DATE D'ENTRÉE EN VIGUEUR :	DATE DE RÉVISION :	REMPLECE LE NUMÉRO :	NOMBRE DE PAGES :
			5
APPLICABLE À :			
Tous les employés, fournisseurs et agents du GN qui utilisent les systèmes de dossiers de santé électroniques.			

1. PRÉAMBULE

La présente directive a pour but de guider les employés, fournisseurs et agents du gouvernement du Nunavut (GN) dans la gestion de la sécurité des informations dans les systèmes de cybersanté, comprenant les dossiers de santé électroniques interopérables (DSEi).

Le ministère de la Santé est assujéti à la Loi sur l'accès à l'information et à la protection de la vie privée (AIPVP), une loi qui a été édictée pour rendre les organismes publics redevables à la population par rapport au traitement des informations et à la protection de la vie privée. Les renseignements personnels sur la santé sont compris dans la définition des renseignements personnels de l'AIPVP.

L'article 42 de l'AIPVP requiert que le ministère de la Santé protège les renseignements personnels « en prenant les mesures de sécurité voulues contre des risques tels que l'accès, la collecte, l'usage, la divulgation et le retrait non autorisés. »

Les clients font confiance au GN et s'attendent à ce que celui-ci protège la confidentialité, l'intégrité et le caractère privé de leurs renseignements personnels. Il est essentiel de satisfaire ces attentes afin de promouvoir la sécurité des clients et gagner leur confiance et leur loyauté.

La présente directive s'appuie sur des normes, des procédures opérationnelles et des directives portant sur des aspects spécifiques.

2. PRINCIPES

1. Les systèmes de cybersanté seront installés et utilisés conformément aux principes suivants :
 - a. la priorité de consolider les services publics en développant les infrastructures en cybersanté qui améliorent et rendent plus efficiente et efficace la gestion des renseignements personnels;
 - b. l'Inuit Qaujimajatuqangit qui consiste en Piliriqatigiinni (travailler ensemble vers un but commun), Inuuqatigiitsiarniq (respecter les autres, les relations et prendre soin des gens), Tunnganarniq (nourrir une bonne attitude en étant ouvert, accueillant et inclusif) et Pilimmaksarniq (acquérir des compétences par la pratique, l'effort et l'action);

- c. le GN, incluant le ministère de la Santé, a l'obligation légale de protéger les renseignements et dossiers personnels qu'il détient en prenant les mesures de sécurité voulues contre les risques tels l'accès, la collecte, l'usage, la divulgation et le retrait non autorisés de tels renseignements;
- d. tous les employés, fournisseurs et agents du GN ont la responsabilité de protéger la confidentialité et le caractère privé des renseignements personnels traités et sauvegardés dans les systèmes de cybersanté, qu'ils proviennent du GN ou de ses clients, fournisseurs en soins de santé ou d'autres sources;
- e. les stratégies, politiques et normes relatives à la gestion de la sécurité des informations dans les systèmes de cybersanté doivent être coordonnées et intégrées conformément à la vision, aux objectifs et aux plans du GN;
- f. les utilisateurs des systèmes de cybersanté doivent avoir conscience de leur responsabilité à l'égard de la sécurité et du caractère privé des renseignements personnels et des systèmes technologiques. Ils doivent aussi savoir ce qu'ils peuvent et doivent faire afin d'assurer la sécurité;
- g. les utilisateurs des systèmes de cybersanté doivent agir de manière prompte et collaborative afin de prévenir et détecter les atteintes à la sécurité, et intervenir;
- h. les risques liés à la sécurité des informations doivent être analysés, traités et surveillés. La haute direction doit prendre des mesures raisonnables pour gérer ces risques;
- i. la sécurité des systèmes et réseaux de cybersanté doit être révisée et réévaluée à intervalles réguliers pour que des modifications appropriées puissent être apportées aux politiques, directives, normes, mesures de protection et procédures.

3. PORTÉE ET APPLICATION

La présente directive relative à la sécurité des informations dans les systèmes de cybersanté s'applique à :

- a. tous les utilisateurs, incluant les employés, fournisseurs et agents du GN qui accèdent aux systèmes de cybersanté, les utilisent, les exploitent ou les entretiennent;
- b. toutes les ressources et informations des systèmes de cybersanté, incluant les renseignements personnels électroniques, les données liées à l'administration et à la sécurité, le matériel, les logiciels, les réseaux et outils de communication;
- c. toutes les activités relatives à l'installation et à l'exploitation des systèmes de cybersanté.

4. RÔLES ET RESPONSABILITÉS

- 1. Le sous-ministre à la Santé :
 - a. a la responsabilité d'administrer toutes les dispositions de la présente directive;
 - b. émet au besoin des directives portant sur des aspects spécifiques des systèmes de cybersanté.
- 2. Le ministère de la Santé :
 - a. est responsable de la sécurité des informations dans les systèmes de cybersanté;
 - b. élabore et met en place un programme de gestion de la sécurité des informations;
 - c. élabore et applique une directive relative à la sécurité des informations dans les systèmes de cybersanté, d'autres directives portant sur des aspects spécifiques ainsi que des procédures opérationnelles pour les systèmes de cybersanté;

- d. est responsable de l'application quotidienne de mesures raisonnables de gestion de la sécurité visant à protéger les renseignements personnels contre l'accès, la collecte, l'usage, la divulgation, la conservation ou le retrait non autorisés, et à garantir l'accessibilité des systèmes de cybersanté.
3. Le ministère des Services communautaires et gouvernementaux :
 - a. est responsable de la mise en œuvre de mesures de sécurité physiques et logiques raisonnables visant à protéger les systèmes de cybersanté, les systèmes connexes et les réseaux de communication hébergés par le GN ou par des tierces parties mandatées par le ministère;
 - b. veille à ce que les systèmes de cybersanté soient configurés et entretenus conformément aux lois, politiques de sécurité, directives, normes et procédures applicables;
 - c. surveille les attaques contre les systèmes de cybersanté par des agents internes ou externes;
 - d. s'assure que les mesures de protection nécessaires sont en place pour protéger les systèmes de cybersanté contre les menaces relevées lors des évaluations des menaces et des risques (EMR);
 - e. a la responsabilité d'élaborer, tester et mettre à jour un plan de reprise après sinistre faisant en sorte que les services de santé soient le moins perturbés possible lorsqu'une défaillance catastrophique du système survient;
 - f. a la responsabilité de détecter et d'investiguer les atteintes à la sécurité, et d'intervenir;
 - g. a la responsabilité de répertorier, d'évaluer et de documenter toutes les ressources des systèmes de cybersanté, y compris les renseignements personnels, les données administratives du système et de la sécurité, le matériel, les logiciels et les outils de communication. En consultation avec le ministère de la Santé, il leur attribue des niveaux de confidentialité et d'importance, et en détermine la propriété.
 4. Les utilisateurs des systèmes de cybersanté :
 - a. ont la responsabilité de préserver la confidentialité des renseignements personnels, de respecter toutes les politiques, directives et procédures de sécurité, et de signaler toute atteinte ou présumée atteinte à la sécurité.

5. PROGRAMME DE GESTION DE LA SÉCURITÉ DES INFORMATIONS

1. Le programme de gestion de la sécurité des informations comprend les éléments suivants :
 - a. mise en place d'un programme d'évaluation des menaces et des risques pour les systèmes de cybersanté et pour gérer les risques identifiés par ce type de programmes;
 - b. formation sur la sécurité et la protection des renseignements personnels pour tous les utilisateurs des systèmes de cybersanté;
 - c. surveillance et audit des accès aux systèmes de cybersanté et de la conformité à la présente directive et aux directives portant sur des aspects spécifiques;
 - d. participation aux enquêtes et aux interventions avec les Services communautaires et gouvernementaux lorsqu'il y a des incidents liés à la sécurité, y compris des tentatives d'accès non autorisés ou des tentatives visant à compromettre un système de cybersanté;
 - e. surveillance de l'état du programme de sécurité et compte rendu à la haute direction;
 - f. conseils continus aux utilisateurs sur des questions relatives à la sécurité des informations;

- g. définition des exigences en matière de sécurité s'appliquant aux services fournis par des organismes (partenaires de programme) qui entretiennent les systèmes de cybersanté, et surveillance de leur conformité à ces exigences, politiques et directives;
- h. établissement d'ententes avec les fournisseurs et les vendeurs de produits et de services qui garantissent leur conformité, tel que requis, à la présente directive relative à la sécurité des informations dans les systèmes de cybersanté, aux directives portant sur des aspects spécifiques, aux normes et aux procédures opérationnelles;
- i. élaboration, mise à l'essai et mise à jour d'un plan de poursuite des activités pour chaque système de cybersanté, assurant la poursuite des services de santé en cas de défaillance du système;
- j. détermination et classification des niveaux de confidentialité des renseignements personnels dans les systèmes de cybersanté, et mise en place de mesures de protection adaptées et proportionnelles à ces niveaux.

6. ACCÈS AUX SYSTÈMES DE CYBERSANTÉ

1. L'accès aux systèmes de cybersanté est basé sur le rôle.
2. Les rôles des utilisateurs et exploitants seront définis par le ministère en consultation avec les parties prenantes. Les utilisateurs et les exploitants se verront attribuer leur rôle par leur superviseur.
3. L'accès aux systèmes de cybersanté et à leurs ressources est accordé en fonction du rôle et des besoins d'information de l'utilisateur.
4. Les activités des utilisateurs, y compris l'accès aux systèmes de cybersanté, peuvent être surveillées et auditées par le ministère de la Santé.

7. VIOLATIONS

1. Tout employé du GN qui commet une violation de la présente directive relative à la sécurité des informations dans les systèmes de cybersanté ou de toute autre directive, norme et procédure opérationnelle portant sur un aspect spécifique connexe est passible de mesures disciplinaires, conformément aux politiques et procédures du GN.
2. Tout fournisseur, commerçant ou contractuel, y compris ses employés et agents, qui commet une violation de la présente directive relative à la sécurité des informations dans les systèmes de cybersanté ou de toute autre directive, norme et procédure opérationnelle portant sur un aspect spécifique connexe est passible des recours prévus dans l'entente ou le contrat. Le ministère de la Santé ou des Services communautaires et gouvernementaux peut exiger le retrait d'un fournisseur, commerçant ou contractuel, ainsi que de ses employés et agents, lorsqu'une telle violation est commise.

8. ADMINISTRATION DE LA PRÉSENTE DIRECTIVE

1. La présente directive est revue par le sous-ministre de la Santé chaque année ou aussitôt qu'une enquête est déclenchée sur une présumée atteinte à la sécurité survenue dans le cadre de la collecte, de l'usage ou de la divulgation non autorisés de renseignements personnels, ou encore lorsque les résultats de l'évaluation ou de l'audit sur la sécurité des informations sont négatifs. Les directives portant sur des aspects spécifiques seront également revues en cas d'atteinte à la sécurité, selon la nature de la violation. Le rapport de révision est remis au ministre de la Santé.

9. AUTORISATION

Sous-ministre adjoint
Ministère de la Santé

Date

Sous-ministre adjoint
Ministère des Services communautaires
et gouvernementaux

Date

 Ministère de la Santé Gouvernement du Nunavut	DIRECTIVE DU MINISTÈRE DE LA SANTÉ		
	DIRECTIVE SUR LA SÉCURITÉ ET LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS LES DSEi		
TITRE :		SECTION :	NUMÉRO DE POLITIQUE :
Directive sur la conservation et le retrait des renseignements personnels électroniques			
DATE D'ENTRÉE EN VIGUEUR :	DATE DE RÉVISION :	REPLACE LE NUMÉRO :	NOMBRE DE PAGES :
			4
APPLICABLE À :			
Tous les employés, fournisseurs et agents du GN qui utilisent les systèmes de dossiers de santé électroniques.			

1. PRÉAMBULE

La présente directive a pour but de guider les employés, fournisseurs et agents du gouvernement du Nunavut (GN) sur les questions relatives à la conservation et au retrait des renseignements personnels électroniques.

Le ministère de la Santé est assujéti à la Loi sur l'accès à l'information et à la protection de la vie privée (AIPVP), une loi qui a été édictée pour rendre les organismes publics redevables à la population par rapport au traitement des informations et à la protection de la vie privée. Les renseignements personnels sur la santé sont compris dans la définition des renseignements personnels de l'AIPVP.

L'article 42 de l'AIPVP requiert que le ministère de la Santé protège les renseignements personnels « en prenant les mesures de sécurité voulues contre des risques tels que l'accès, la collecte, l'usage, la divulgation et le retrait non autorisés. »

Les clients font confiance au GN et s'attendent à ce que celui-ci protège la confidentialité, l'intégrité et le caractère privé de leurs renseignements personnels. Il est essentiel de satisfaire ces attentes afin de promouvoir la sécurité des clients et gagner leur confiance et leur loyauté.

2. PRINCIPES

1. Le ministère de la Santé conserve et retire les renseignements personnels conformément aux principes suivants :
 - a. la priorité de consolider les services publics en développant les infrastructures en cybersanté qui améliorent et rendent plus efficace et efficace la gestion des renseignements personnels;
 - b. l'*Inuit Qaujimajatuqangit* qui consiste en *Piliriqatigiinniq* (travailler ensemble vers un but commun), *Inuuqatigiitsiarniq* (respecter les autres, les relations et prendre soin des gens), *Tunnganarniq* (nourrir une bonne attitude en étant ouvert, accueillant et inclusif) et *Pilimmaksarniq* (acquérir des compétences par la pratique, l'effort et l'action);
 - c. le GN, incluant le ministère de la Santé, a l'obligation légale de protéger les renseignements et dossiers personnels qu'il détient en prenant les mesures de sécurité voulues contre les risques tels l'accès, la collecte, l'usage, la divulgation et le retrait non autorisés de tels renseignements;

- d. les renseignements personnels électroniques sont conservés conformément aux exigences de la Loi sur les archives et l'AIPVP;
- e. les renseignements personnels électroniques sont conservés pour une durée qui convient aux fins pour lesquelles ils ont été collectés;
- f. les renseignements personnels sont détruits ou rendus anonymes à l'expiration de la période de conservation, conformément aux exigences de la Loi sur les archives;
- g. les supports contenant des renseignements personnels qui ne sont plus requis seront détruits dans leur entièreté et de manière sécuritaire.

3. PORTÉE ET APPLICATION

1. La présente directive portant sur la conservation et le retrait des renseignements personnels électroniques s'applique à :
 - a. tous les employés, contractuels et agents du GN ainsi que tous les vendeurs et fournisseurs de produits et services au GN qui accèdent aux systèmes de cybersanté, les utilisent, les exploitent ou les entretiennent;
 - b. tous les renseignements personnels sous forme électronique, les données de production (données se trouvant dans les dossiers actifs), les données archivées, les copies de sauvegarde des données (en cas de défaillance pour assurer la poursuite des activités), les journaux d'audit contenant des renseignements personnels et les copies des données créées à des fins autorisées;
 - c. tous les logiciels et données essentielles du système de sécurité requis pour accéder aux renseignements personnels se trouvant sur support électronique.

4. RÔLES ET RESPONSABILITÉS

1. Le Comité des documents publics du GN a la responsabilité générale d'approuver les calendriers de conservation et les méthodes de retrait des documents publics en vertu de la Loi sur les archives.
2. Le ministère de la Santé a la responsabilité première de la conservation et du retrait des renseignements personnels électroniques dans les systèmes de cybersanté.
3. Le ministère des Services communautaires et gouvernementaux maintient la responsabilité de la sécurité des renseignements personnels contenus dans les systèmes et installations, y compris en ce qui concerne le retrait et la destruction sécuritaires de ces renseignements et de leurs supports.

5. CONSERVATION DES RENSEIGNEMENTS PERSONNELS

1. Conformément à l'autorisation de disposer de documents (ADD) 2005-3, les renseignements personnels électroniques sont conservés pour une période de 20 ans suivant la date de la dernière entrée, la date de décès de l'individu ou la date à laquelle il a atteint l'âge de la majorité. Cela ne s'applique pas aux copies de sauvegarde des bases de données de renseignements personnels créées pour la récupération et la poursuite des activités en cas de défaillance et pour les journaux d'audit contenant des renseignements personnels.
2. En conformité avec la version révisée 2007-01 de l'ADD 1995-32 (système de classification des documents administratifs), les ministères de la Santé et des Services communautaires et gouvernementaux établissent des calendriers de conservation pour les copies de sauvegarde des bases de données de renseignements personnels créées pour la récupération et la poursuite des activités en cas de défaillance, pour les journaux d'audit contenant des renseignements personnels et à d'autres fins autorisées. Ces calendriers sont basés sur une évaluation des besoins opérationnels.
3. Le ministère de la Santé garde un inventaire de toutes les bases de données et tous les

dépôts de renseignements personnels électroniques, y compris les copies de sauvegarde créées pour la récupération et la poursuite des activités en cas de défaillance, pour les journaux d'audit contenant des renseignements personnels et à d'autres fins autorisées.

4. Les utilisateurs ne peuvent pas copier ou télécharger de renseignements personnels à partir des systèmes de cybersanté sans l'autorisation du ministère de la Santé. Le ministère établira une entente avec les utilisateurs qui téléchargent des données à des fins autorisées et conservera un registre des données téléchargées, leur emplacement, la personne responsable de leur protection et leurs modalités de conservation et de retrait.
5. Les Services communautaires et gouvernementaux s'assurent que tout logiciel, tout matériel ou tout utilitaire (par ex. : programme d'encodage) utilisé pour lire ou copier des renseignements personnels archivés ou sauvegardés reste disponible pendant toute la période de conservation des renseignements.
6. Lorsque survient un changement technologique (par ex. une nouvelle version d'un logiciel), les Services communautaires et gouvernementaux s'assurent que la nouvelle technologie puisse déchiffrer les données de production et données archivées. Dans le cas contraire, les Services convertiront les données dans un format compatible avec la nouvelle technologie.
7. Si des données de production et des données archivées sont cryptées, les Services s'assureront que les programmes de décryptage, les algorithmes et les clés requis pour les décrypter seront accessibles durant toute la période de conservation, et maintenus dans un endroit sécuritaire.
8. Les ministères de la Santé et des Services communautaires et gouvernementaux mettront en place les mesures de contrôle nécessaires pour protéger les renseignements personnels contre la perte, la destruction et la falsification, en conformité avec la présente directive.

6. CRÉATION ET CONSERVATION DE COPIES DE SAUVEGARDE

1. Les ministères de la Santé et des Services communautaires et gouvernementaux établissent un calendrier de sauvegarde des données pour qu'elles puissent être récupérées en cas de défaillance.
2. Le plan de récupération fournit des détails sur les données devant être sauvegardées aux fins de récupération en cas de défaillance, y compris les renseignements personnels, les logiciels d'application et les données essentielles du système de sécurité.
3. Les supports contenant des données sauvegardées sont stockés dans un lieu sûr, séparé du lieu de stockage principal (par ex., à part des données de production et des données archivées).
4. Les bandes magnétiques et autres supports de sauvegarde contenant des données comme les renseignements personnels, les logiciels d'application et les données essentielles du système de sécurité peuvent être recyclés et réutilisés après que leur contenu ait été supprimé de manière sécuritaire. Les ministères de la Santé et des Services communautaires et gouvernementaux déterminent et documentent selon une certaine procédure les méthodes utilisées pour le nettoyage des supports de sauvegarde.

7. RETRAIT ET ÉLIMINATION DES RENSEIGNEMENTS PERSONNELS

1. À la fin de leur période de conservation, les renseignements personnels qui ne sont plus requis aux fins pour lesquelles ils ont été collectés sont détruits ou rendus anonymes, de même que leurs copies.
2. En collaboration avec les Services communautaires et gouvernementaux, le ministère de

la Santé doit obtenir une autorisation écrite du Comité des documents publics avant de détruire ou de supprimer tout fichier électronique contenant des renseignements personnels.

3. Un algorithme ou un programme d'anonymisation ou de pseudonymisation est utilisé pour rendre les renseignements personnels anonymes. Une fois le processus d'anonymisation ou de pseudonymisation terminé, les fichiers sources sont supprimés de manière sécuritaire.
4. Les ministères de la Santé et des Services communautaires et gouvernementaux déterminent et documentent selon une certaine procédure les méthodes utilisées pour détruire ou supprimer de manière permanente des supports contenant des renseignements personnels, des logiciels d'application ou des données essentielles du système de sécurité.
5. Lorsqu'ils ne sont plus requis, les supports contenant des renseignements personnels, des logiciels d'application ou des données essentielles du système de sécurité sont détruits en totalité et de façon sécuritaire, ou effacés de manière permanente.
6. Lorsque des équipements ou des dispositifs (par ex.: disque dur, clé USB) comprenant des renseignements personnels, des logiciels d'application ou des données essentielles du système de sécurité sont envoyés pour être réparés, réutilisés ou supprimés, ces informations doivent d'abord être supprimées, détruites ou effacées de manière permanente.

8. ADMINISTRATION DE LA PRÉSENTE DIRECTIVE

La présente directive est revue chaque année par les sous-ministres de la Santé et des Services communautaires et gouvernementaux ou dès qu'une enquête est déclenchée sur une présumée violation de la sécurité relative à la conservation ou au retrait des renseignements personnels, ou lorsqu'un audit de sécurité ou une évaluation des menaces et des risques portant sur la conservation ou le retrait des renseignements personnels mène à des résultats négatifs. Le rapport de révision est remis aux ministres de la Santé et des Services communautaires et gouvernementaux.


9. AUTORISATION

Sous-ministre
Ministère de la Santé

Date

Sous-ministre
Ministère des Services communautaires
et gouvernementaux

Date

 Ministère de la Santé Gouvernement du Nunavut	DIRECTIVE DU MINISTÈRE DE LA SANTÉ		
	DIRECTIVE SUR LA SÉCURITÉ ET LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS LES DSEi		
TITRE :		SECTION :	NUMÉRO DE POLITIQUE :
Directive sur la protection des renseignements personnels dans les systèmes de cybersanté			
DATE D'ENTRÉE EN VIGUEUR :	DATE DE RÉVISION :	REPLACE LE NUMÉRO :	NOMBRE DE PAGES :
			6
APPLICABLE À :			
Tous les employés, fournisseurs et agents du GN qui utilisent les systèmes de cybersanté.			

1. PRÉAMBULE

La présente directive a pour but de guider les employés, fournisseurs et agents du gouvernement du Nunavut (GN) quant à la protection des renseignements personnels dans le cadre d'initiatives de cybersanté, comme les dossiers de santé électroniques interopérables (DSEi).

Le ministère de la Santé est assujéti à la Loi sur l'accès à l'information et à la protection de la vie privée (AIPVP), une loi qui a été édictée pour rendre les organismes publics redevables à la population par rapport au traitement des informations et à la protection de la vie privée. Les renseignements personnels sur la santé sont compris dans la définition des renseignements personnels de l'AIPVP.

Les clients font confiance au GN et s'attendent à ce que celui-ci protège la confidentialité, l'intégrité et le caractère privé de leurs renseignements personnels. Il est essentiel de satisfaire ces attentes afin de promouvoir la sécurité des clients et gagner leur confiance et leur loyauté.

La présente directive s'appuie sur des normes, des procédures opérationnelles et des directives portant sur des aspects spécifiques.

2. PRINCIPES

1. Les systèmes de cybersanté seront installés et utilisés conformément aux principes suivants :
 - a. la priorité de consolider les services publics en développant les infrastructures en cybersanté qui améliorent et rendent plus efficiente et efficace la gestion des renseignements personnels;
 - b. l'*Inuit Qaujimajatuqangit* qui consiste en *Piliriqatigiinniq* (travailler ensemble vers un but commun), *Inuuqatigiitsiarniq* (respecter les autres, les relations et prendre soin des gens), *Tunnganarniq* (nourrir une bonne attitude en étant ouvert, accueillant et inclusif) et *Pilimmaksarniq* (acquérir des compétences par la pratique, l'effort et l'action);
 - c. le GN, incluant le ministère de la Santé, a l'obligation légale de protéger les renseignements et dossiers personnels qu'il détient en prenant les mesures de sécurité voulues contre les risques tels l'accès, la collecte, l'usage, la divulgation et le retrait non autorisés de tels renseignements;

- d. chaque personne a fondamentalement besoin d'intimité et a juridiquement le droit de contrôler la possession, l'usage et la divulgation de ses renseignements personnels;
- e. les renseignements personnels ne doivent être recueillis, utilisés et communiqués que par des personnes autorisées, conformément à l'AIPVP, aux autres lois et règlements applicables, aux politiques du GN et aux politiques et directives du ministère de la Santé à l'égard de la vie privée et de la protection des renseignements personnels.

3. PORTÉE ET APPLICATION

1. La présente Directive sur la protection des renseignements personnels dans les systèmes de cybersanté s'applique à :
 - a. tous les employés, fournisseurs et agents du GN qui accèdent aux systèmes de cybersanté, les utilisent, les opèrent ou les entretiennent;
 - b. tous les renseignements personnels récoltés, utilisés, communiqués et conservés par le GN dans les systèmes de cybersanté.

4. IMPUTABILITÉ

1. Le ministre de la Santé :
 - a. a délégué au sous-ministre de la Santé le pouvoir de collecter, d'utiliser et de communiquer les renseignements personnels, et ce, en vertu de l'AIPVP. Par conséquent, le sous-ministre a la responsabilité de mettre en pratique toutes les dispositions figurant dans la présente directive.
2. Le sous-ministre à la Santé :
 - a. instaure et maintient un programme d'accès à l'information et de protection des renseignements personnels;
 - b. élabore et met à jour des directives portant sur des aspects spécifiques ainsi que des procédures opérationnelles relatives aux systèmes de cybersanté;
 - c. est responsable de la protection des renseignements personnels qui sont consultés, recueillis, utilisés, communiqués, stockés et conservés dans les systèmes de cybersanté, qu'ils soient générés par le ministère ou transmis à celui-ci par des clients, des fournisseurs de soins de santé ou d'autres sources;
 - d. s'assure que tous les agents à qui le ministère a transmis des renseignements personnels à des fins de traitement ou de manipulation sont tenus, par voie d'un engagement contractuel, à respecter un niveau comparable de protection lors du traitement ou de la manipulation de ces renseignements.
3. Les utilisateurs des systèmes de cybersanté :
 - a. ont la responsabilité de protéger en tout temps la confidentialité et le caractère privé des renseignements personnels utilisés ou communiqués dans l'exercice de leurs fonctions;
 - b. doivent agir de manière prompte et collaborative pour prévenir, détecter et rapporter toute violation de la vie privée.

5. BUTS DE LA COLLECTE

1. Le ministère de la Santé doit préciser au client à quelles fins il collecte, utilise ou communique ses renseignements personnels et en vertu de quel pouvoir juridique précis. Le ministère doit également informer le client du titre, des coordonnées professionnelles et du numéro de téléphone de la personne à contacter au sujet de la collecte, de l'usage, de la divulgation et de la conservation de ses renseignements personnels dans les systèmes de cybersanté.

2. Le ministère de la Santé ne peut pas utiliser les renseignements personnels à d'autres fins que celles stipulées. Tout nouvel usage qui n'est pas prévu par la loi doit être autorisé par écrit par le client.

6. CONSENTEMENT

1. En vertu de l'AIPVP, la collecte, l'usage et la divulgation des renseignements personnels requièrent le consentement oral ou écrit du client concerné. Celui-ci doit préciser à qui ces informations peuvent être communiquées et comment elles peuvent être utilisées. De plus, son consentement doit être éclairé, c'est-à-dire qu'il doit être raisonnable de présumer dans les circonstances que le client :
 - a. connaît les fins pour lesquelles ses renseignements sont recueillis, utilisés ou communiqués;
 - b. sait qu'il a le choix de donner ou non son consentement.
2. Lorsque le consentement requis ci-dessus à la clause 1 est accordé oralement, le ministère doit dès que possible produire et conserver une trace écrite de ce consentement.

7. LIMITATIONS EN MATIÈRE DE COLLECTE DES RENSEIGNEMENTS PERSONNELS

1. Le ministère ne peut pas collecter des renseignements personnels de manière injustifiée. La quantité et le type d'informations demandées doivent se limiter à ce qui est nécessaire aux fins stipulées.
2. Les renseignements personnels ne peuvent être obtenus que de manière légale. Les clients ne doivent pas être induits en erreur ou trompés en ce qui a trait aux fins pour lesquelles les informations sont recueillies.

8. LIMITATIONS EN MATIÈRE D'USAGE, DE DIVULGATION ET DE CONSERVATION DES RENSEIGNEMENTS PERSONNELS

1. Les renseignements personnels ne doivent pas être utilisés ou communiqués à des fins autres que celles pour lesquelles ils ont été recueillis ou d'une manière qui ne soit pas conforme à celles-ci, sauf avec le consentement écrit du client.
2. Les renseignements personnels qui ne sont plus requis aux fins stipulées doivent être retirés ou rendus anonymes. La conservation des dossiers électroniques de renseignements personnels est assujettie aux exigences légales et réglementaires. Elle doit se faire conformément aux dispositions applicables à la conservation et au retrait des renseignements personnels électroniques dans la Directive sur la sécurité et la protection des renseignements personnels dans les DSEi.

9. EXACTITUDE

1. Le ministère de la Santé doit prendre des mesures raisonnables pour s'assurer que les renseignements personnels sont exacts, complets et à jour de manière à éliminer ou minimiser le risque qu'une décision soit basée sur une information inexacte au sujet d'un client.
2. Si un renseignement personnel est incomplet ou inexact, ou si un client démontre que ses renseignements personnels sont incomplets ou inexacts, le ministère de la Santé s'assurera que les informations soient corrigées ou inscrira une note dans le dossier de santé du client concerné réclamant que la correction soit effectuée.
3. Les informations contenues dans le dossier de santé du client ne peuvent pas être effacées. Les informations initiales sont conservées de manière à ce que toutes les modifications ou corrections soient visibles.

4. Le ministère de la Santé informe les instances publiques et tierces parties ayant obtenu les renseignements personnels dans les douze mois précédant la demande de correction que ces renseignements ont été modifiés ou qu'une note réclamant qu'une correction soit effectuée a été ajoutée dans le dossier de santé du client concerné.

10. MESURES DE PROTECTION

1. Le ministère de la Santé s'assure que des mesures de protection physiques, administratives et techniques appropriées sont mises en place afin de prévenir la perte, le vol, l'accès non autorisé, l'usage, la divulgation, la copie et la modification des renseignements personnels.

11. TRANSPARENCE

1. Le ministère de la Santé produit un avis écrit s'adressant aux clients et au public qui :
 - a. fournit une description générale des pratiques relatives au traitement des renseignements au ministère;
 - b. explique comment contacter la personne responsable de la protection des renseignements recueillis, utilisés, communiqués, stockés et conservés dans les systèmes de cybersanté;
 - c. explique comment un client peut avoir accès à son dossier de renseignements personnels ou demander que des corrections y soient apportées;
 - d. explique comment un client peut déposer une plainte relativement au traitement de ses renseignements personnels;
 - e. utilise un langage simple et respecte les lois linguistiques du Nunavut.
2. Cet avis public doit être affiché dans tous les établissements où le ministère de la Santé collecte des renseignements personnels, à un endroit aisément visible par la clientèle.

12. ACCÈS INDIVIDUEL

1. Les clients peuvent accéder sous supervision à leurs renseignements personnels ou à une copie de ceux-ci, après avoir remis un formulaire d'autorisation signé ou une autre forme de requête écrite¹ acceptée, sauf si le ministère détermine qu'il est raisonnable de croire que l'accès à ces renseignements porte une atteinte grave et immédiate à la santé et à la sécurité mentales et physiques de l'individu.
2. Sur demande, le ministère de la Santé fournit au client une liste de toutes les tierces parties à qui ses renseignements personnels ont été communiqués. S'il n'est pas en mesure de fournir une telle liste, le ministère doit transmettre une liste des tierces parties à qui il est susceptible d'avoir communiqué ces informations.
3. Le ministère de la Santé répond promptement à la demande du client d'accéder à ses renseignements personnels, ainsi qu'à toute demande de correction ou de modification, conformément aux lois applicables.
4. Le ministère de la Santé peut exiger des frais aux individus qui souhaitent obtenir des copies de leurs renseignements personnels, conformément aux lois applicables.

13. PLAINTES

1. Le ministère de la Santé met en place des procédures visant à recevoir les plaintes et les requêtes reliées à ses politiques, ses directives et ses pratiques de traitement des renseignements personnels dans les systèmes de cybersanté, et à y donner suite.

¹ Un client peut faire une demande d'accès orale lorsque sa capacité à lire ou à écrire une des langues officielles est limitée, ou lorsqu'une incapacité physique ou une condition particulière affecte sa capacité à écrire sa demande.

2. Le ministère de la Santé déploiera un effort raisonnable afin d'examiner chaque plainte. Si une plainte s'avère justifiée, le ministère prendra les mesures appropriées pour régler la plainte et réduire les risques qu'elle se reproduise.

14. PROGRAMME D'ACCÈS À L'INFORMATION

1. Le programme d'accès à l'information prévoit :
 - a. des mesures veillant au respect de l'AIPVP et de toute autre loi applicable reliée à la collecte, l'usage, la divulgation et la protection des renseignements personnels;
 - b. des formations pour les employés et contractuels du GN portant sur la confidentialité et la sécurité;
 - c. un processus de réception, d'examen et de résolution des questions ou des plaintes;
 - d. un volet de surveillance et d'audit des accès aux dossiers de renseignements personnels dans les DSEi et les autres systèmes de cybersanté. Ce volet vise la détection des atteintes à la sécurité ou à la vie privée et veille au respect de l'AIPVP et des autres lois applicables, ainsi que des directives du ministère quant à la sécurité et la protection des renseignements personnels dans les DSEi;
 - e. un processus de réponse aux violations potentielles de la vie privée qui soit conforme à l'AIPVP, incluant l'envoi d'une notification au commissaire à l'accès à l'information et à la protection de la vie privée ainsi qu'au client s'il y a lieu;
 - f. l'ouverture d'enquêtes dans les cas de violations de la vie privée et l'émission de recommandations adressées à la haute direction quant à des mesures correctives à entreprendre;
 - g. la création ou l'encadrement de la création d'évaluations mesurant les répercussions sur la vie privée des systèmes de cybersanté et des infrastructures du GN;
 - h. du matériel de communication pour le public;
 - i. des directives pour les gestionnaires ministériels qui rédigent les ententes et les contrats avec des tierces parties requérant l'accès aux renseignements personnels;
 - j. des directives pour le personnel médical et les gestionnaires ministériels sur la gestion des demandes d'accès et de correction des clients visant leurs dossiers de santé papier et électroniques.

15. VIOLATIONS

1. Tout employé du GN qui commet une violation de la présente Directive sur la protection des renseignements personnels dans les systèmes de cybersanté ou de toute autre directive, norme et procédure portant sur un aspect spécifique connexe est passible de mesures disciplinaires, conformément aux politiques et procédures du GN.
2. Tout fournisseur, commerçant ou contractuel, incluant ses employés et agents, qui commet une violation de la présente Directive sur la protection des renseignements personnels dans les systèmes de cybersanté ou de toute autre directive, norme et procédure portant sur un aspect spécifique connexe est passible des recours prévus dans l'entente ou le contrat. Le ministère de la Santé peut exiger le retrait d'un fournisseur, commerçant ou contractuel, ainsi que de ses employés et agents, lorsqu'une telle violation est commise.


16. ADMINISTRATION DE LA PRÉSENTE DIRECTIVE

La présente directive est revue par le sous-ministre de la Santé chaque année ou aussitôt qu'une enquête est déclenchée sur une présumée violation de la vie privée ayant été commise dans le cadre de la collecte, de l'usage ou de la divulgation autorisée de renseignements personnels, ou encore lorsque les résultats de l'évaluation ou de l'audit sont négatifs. Les directives portant sur des aspects spécifiques connexes seront également revues dans le cas d'une violation de la vie privée, suivant la nature de la violation. Le rapport de révision est remis au ministre de la Santé.

17. AUTORISATION

Sous-ministre
Ministère de la Santé

Date

 Ministère de la Santé Gouvernement du Nunavut	DIRECTIVE DU MINISTÈRE DE LA SANTÉ		
	DIRECTIVE SUR LA SÉCURITÉ ET LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS LES DSEi		
TITRE :		SECTION :	NUMÉRO DE POLITIQUE :
Gestion des mots de passe dans les systèmes de cybersanté			
DATE D'ENTRÉE EN VIGUEUR :	DATE DE RÉVISION :	REPLACE LE NUMÉRO :	NOMBRE DE PAGES :
			3
APPLICABLE À :			
Tous les employés, fournisseurs et agents du GN qui utilisent les systèmes de dossiers de santé électroniques.			

1. PRÉAMBULE

La présente directive a pour but de guider les employés, fournisseurs et agents du gouvernement du Nunavut (GN) sur les questions relatives à la gestion des mots de passe dans les systèmes de cybersanté, notamment les dossiers de santé électroniques interopérables (DSEi).

Le ministère de la Santé est assujéti à la Loi sur l'accès à l'information et à la protection de la vie privée (AIPVP), une loi qui a été édictée pour rendre les organismes publics redevables à la population par rapport au traitement des informations et à la protection de la vie privée. Les renseignements personnels sur la santé sont compris dans la définition des renseignements personnels de l'AIPVP.

L'article 42 de l'AIPVP requiert que le ministère de la Santé protège les renseignements personnels « en prenant les mesures de sécurité voulues contre des risques tels que l'accès, la collecte, l'usage, la divulgation et le retrait non autorisés. »

Les clients font confiance au GN et s'attendent à ce que celui-ci protège la confidentialité, l'intégrité et le caractère privé de leurs renseignements personnels. Il est essentiel de satisfaire ces attentes afin de promouvoir la sécurité des clients et gagner leur confiance et leur loyauté.

2. PRINCIPES

1. Le ministère de la santé gère et contrôle les mots de passe donnant accès aux systèmes de cybersanté conformément aux principes suivants :
 - a. la priorité de consolider les services publics en développant les infrastructures en cybersanté qui améliorent et rendent plus efficiente et efficace la gestion des renseignements personnels;
 - b. l'*Inuit Qaujimajatuqangit* qui consiste en *Piliriqatigiinni* (travailler ensemble vers un but commun), *Inuuqatigiitsiarniq* (respecter les autres, les relations et prendre soin des gens), *Tunnganarniq* (nourrir une bonne attitude en étant ouvert, accueillant et inclusif) et *Pilimmaksarniq* (acquérir des compétences par la pratique, l'effort et l'action);
 - c. le GN, incluant le ministère de la Santé, a l'obligation légale de protéger les renseignements et dossiers personnels qu'il détient en prenant les mesures de

- sécurité voulues contre les risques tels l'accès, la collecte, l'usage, la divulgation et le retrait non autorisés de tels renseignements;
- d. chaque employé et fournisseur du GN qui a accès aux systèmes de cybersanté ou aux ressources des systèmes connexes est responsable de la protection et de l'utilisation de son ou de ses mots de passe;
 - e. chaque employé et fournisseur du GN qui a accès aux systèmes de cybersanté ou aux ressources des systèmes connexes prend des mesures raisonnables pour protéger son ou ses mots de passe, en conformité avec la présente directive;
 - f. toutes les activités des utilisateurs, incluant l'accès aux systèmes de cybersanté, peuvent être surveillées et auditées par le GN.

3. PORTÉE ET APPLICATION

La présente directive sur la gestion des mots de passe dans les systèmes de cybersanté s'applique à :

1. tous les employés, contractuels et agents du GN, ainsi que tous les vendeurs et fournisseurs de produits et services au GN qui accèdent aux systèmes de cybersanté, les utilisent, les exploitent ou les entretiennent;
2. tous les systèmes de cybersanté et aux ressources des systèmes connexes, incluant :
 - a. les données confidentielles :
 - i. renseignements personnels;
 - ii. journaux d'audit des systèmes;
 - iii. données administratives du système et de la sécurité (par ex. configurations de la sécurité technique, informations de mots de passe et d'authentification);
 - b. le matériel comme les appareils mobiles et l'équipement de réseautique;
 - c. les logiciels;
 - d. les ressources en communication et réseautique.

4. GESTION DES MOTS DE PASSE

1. Les utilisateurs des systèmes de cybersanté sont tenus de protéger la confidentialité de leurs mots de passe personnels et de ne pas partager les mots de passe des groupes dont ils font partie.
2. La communication délibérée de mots de passe personnels est considérée comme une violation de la sécurité de la part de l'utilisateur, et fera l'objet d'une enquête et d'un rapport de la part des autorités concernées.
3. Les utilisateurs reçoivent un mot de passe temporaire sécurisé qui doit être changé lors de la première connexion, ou lorsque leur mot de passe est remplacé ou réinitialisé.
4. L'identité des utilisateurs est contrôlée avant qu'ils ne puissent obtenir un nouveau mot de passe ou un mot de passe temporaire.
5. Les mots de passe temporaires sont communiqués aux utilisateurs de manière sécuritaire.
6. Les mots de passe temporaires doivent être uniques et impossibles à deviner.
7. Les mots de passe ne doivent pas être sauvegardés dans un système informatique de manière non protégée.
8. Les mots de passe par défaut des fournisseurs sont modifiés après l'installation des systèmes ou des logiciels.
9. Lorsqu'un employé, un fournisseur ou une tierce partie qui connaît des mots de passe de comptes actifs (par ex., comptes de groupe) quitte, les mots de passe doivent être changés dès que le contrat de travail ou l'entente prend fin.
10. La durée de vie maximale de tout mot de passe ne doit pas excéder 90 jours, après quoi, il doit être changé. Les systèmes sont configurés de manière à réclamer un

changement de mot de passe après 90 jours, ou avant si le directeur des technologies de l'information le détermine ainsi.

11. Un mot de passe ne peut être réutilisé avant au moins 24 changements consécutifs.
12. Tous les nouveaux mots de passe doivent contenir :
 - a. huit caractères ou plus;
 - b. lettre(s) majuscule(s) sans accent (A à Z);
 - c. lettre(s) minuscule(s) sans accent (a à z);
 - d. chiffre(s) (0 à 9);
 - e. un symbole non alphanumérique (comme!, \$, #, %).
13. Le mot de passe ne doit pas contenir le nom du compte, ni le nom complet de l'utilisateur ou plus de trois lettres consécutives de son nom.
14. Tous les mots de passe sont sensibles à la casse.

5. ADMINISTRATION DE LA PRÉSENTE DIRECTIVE

La présente directive est revue chaque année par les sous-ministres de la Santé et des Services communautaires et gouvernementaux ou dès qu'une enquête est déclenchée sur la gestion des mots de passe ou encore lorsque l'évaluation des menaces et des risques ou l'audit de sécurité portant sur la gestion des mots de passe mène à des résultats négatifs. Le rapport de révision est remis aux ministres de la Santé et des Services communautaires et gouvernementaux.


6. AUTORISATION

Sous-ministre
Ministère de la Santé

Date

Sous-ministre
Ministère des Services communautaires
et gouvernementaux

Date

 Ministère de la Santé Gouvernement du Nunavut	DIRECTIVE DU MINISTÈRE DE LA SANTÉ		
	DIRECTIVE DE SÉCURITÉ ET DE PROTECTION DE LA VIE PRIVÉE RELATIVE AU DOSSIER DE SANTÉ ÉLECTRONIQUE INTEROPÉRABLE (DSEi)		
TITRE	ARTICLE	N^o DE POLITIQUE	
Collecte, utilisation et divulgation de renseignements personnels de systèmes de cybersanté			
DATE D'ENTRÉE EN VIGUEUR	DATE D'ÉCHÉANCE DE LA RÉVISION	NUMÉRO REMPLACÉ	NOMBRE DE PAGES
			6
PERSONNES VISÉES			
Employés, entrepreneurs et mandataires du gouvernement du Nunavut utilisant un système de cybersanté			

1. PRÉAMBULE

La présente directive vise à guider les employés, les entrepreneurs et les mandataires du gouvernement du Nunavut (GN) pour la collecte, l'utilisation et la divulgation de renseignements personnels de systèmes de cybersanté, dont le système de dossiers de santé électroniques interopérables (DSEi).

Le ministère de la Santé (« le Ministère ») est assujéti à la Loi sur l'accès à l'information et la protection de la vie privée (LAIPVP), adoptée pour responsabiliser les organismes publics envers la population quant au traitement de l'information et à la protection de la vie privée. Les renseignements personnels, au sens de la LAIPVP, comprennent les renseignements personnels sur la santé.

Les clients comptent sur le Ministère pour préserver la confidentialité, le caractère privé et l'intégrité de leurs renseignements personnels. Il est essentiel de se montrer digne de ces attentes pour assurer la sécurité des clients et conserver leur confiance et leur loyauté.

2. PRINCIPES

1. La collecte, l'utilisation et la divulgation de renseignements personnels par le Ministère suit les principes suivants :

- a) Le renforcement prioritaire de la fonction publique par l'amélioration de l'infrastructure de cybersanté pour une gestion améliorée, plus efficace et plus efficace des renseignements personnels.
- b) Les principes Inuit qaujimajatuqangit de Piliriqatigiinniq (collaborer dans un but commun), Inuuqatigiitsiarniq (respecter l'autre, les rapports avec celui-ci et le souci de son bien-être), Tunnganarniq (promouvoir un bon état d'esprit en étant ouvert, accueillant et rassembleur) et Pilimmaksarniq (développer des compétences par la pratique, l'effort et l'action).
- c) Le GN, dont le Ministère, est tenu par la loi de mettre en œuvre des mesures raisonnables de protection des renseignements personnels en encadrant la collecte, l'utilisation, la divulgation et la suppression des renseignements et des dossiers qui relève de lui, ainsi que l'accès à ceux-ci.
- d) Parmi les besoins fondamentaux de chacun figure le respect de sa vie privée et un droit de décision sur la collecte, l'utilisation et la divulgation de ses renseignements personnels.
- e) Les renseignements personnels sont recueillis, utilisés et divulgués seulement par les personnes autorisées et conformément à la LAIPVP, aux autres lois

applicables et aux politiques et directives en matière de confidentialité et de sécurité des renseignements personnels.

3. CHAMP D'APPLICATION

1. La présente directive vise :
 - a) Le personnel, les entrepreneurs et les mandataires du GN qui se servent ou s'occupent du soutien d'un système de cybersanté.
 - b) Tous les renseignements personnels recueillis, utilisés, divulgués et conservés par le GN dans un système de cybersanté.

4. COLLECTE DE RENSEIGNEMENTS PERSONNELS

1. Les renseignements personnels sont recueillis strictement aux fins autorisées par la LAIPVP ou par d'autres lois applicables.
2. Les clients sont informés par avis public écrit des fins de la collecte au plus tard au moment où elle s'effectue.
3. Le Ministère, en collaboration avec le ministère de la Justice, est saisi des demandes de collecte de renseignements personnels non autorisées par la loi. Si le sous-ministre fait droit à la requête, une marche à suivre est élaborée pour obtenir au préalable le consentement exprès du client conformément aux lois applicables.

5. UTILISATION DES RENSEIGNEMENTS PERSONNELS

1. Le Ministère utilise des renseignements personnels tirés de systèmes de cybersanté pour fournir des services et exécuter des programmes dans les grandes catégories que sont les soins de courte durée, les soins de base, la santé publique, la santé de la population, la prévention et la santé mentale. Ces renseignements sont aussi utilisés pour la planification et la gestion générales du système de santé.
2. Un fournisseur de soins de santé faisant partie du cercle de soins d'un client peut demander l'accès aux renseignements personnels de ce dernier, à condition de le suivre au moment de la demande, et que les renseignements divulgués soient directement liés au domaine de spécialité du fournisseur.
 - a) « Cercle de soins » désigne les médecins, le personnel infirmier, les professionnels paramédicaux et les spécialistes qui traitent le client au moment de la demande.
3. Les renseignements personnels ne peuvent être utilisés à aucune autre fin sauf conformément à la LAIPVP ou à une autre loi applicable.
4. Le Ministère examine toutes les requêtes d'utilisation de renseignements personnels à une fin non autorisée par la loi. Si le sous-ministre fait droit à la requête, une marche à suivre est élaborée pour obtenir au préalable le consentement exprès du client.

6. DIVULGATION DES RENSEIGNEMENTS PERSONNELS

1. Les renseignements personnels ne sont divulgués que par un processus sécurisé ayant reçu la sanction du sous-ministre de la Santé.
2. Le Ministère consigne toute divulgation dans le dossier du client en indiquant avec précision l'objet, les fins, le destinataire et le destinataire de la divulgation.
3. Le Ministère voit à la confirmation de l'identité du destinataire de toute divulgation, nonobstant toute confirmation antérieure¹.

¹ Voir le Règlement sur l'accès à l'information et la protection de la vie privée, article 5(4), au sujet des pièces d'identité devant être produites pour demander la divulgation de renseignements personnels ou y consentir.

4. Toute divulgation de renseignements personnels non visée par la colonne « Divulgation autorisée » ci-dessous doit au préalable faire l'objet du consentement exprès du client, notamment lorsqu'elle est destinée aux membres de sa famille, à ses amis, à un employeur, à une compagnie d'assurance ou à un avocat².
5. Toute divulgation autorisée nécessite une autorisation écrite, sauf celles faites au sein du cercle de soins du client, les avis au plus proche parent, les autorisations donnant accès à des services de santé assurés et les divulgations faites au registraire des registres des maladies. Le requérant doit indiquer dans sa demande, outre ses fins, l'autorité législative sur laquelle il s'appuie.
6. Toute divulgation de renseignements personnels doit se limiter à ce que les fins autorisées justifient raisonnablement.
7. Divulgations autorisées – Le tableau ci-dessous présente sommairement les divulgations autorisées par la LAIPVP ou par une autre loi applicable sans le consentement exprès du client. **LES DIVULGATIONS AUTORISÉES DOIVENT TOUT DE MÊME SE FAIRE CONFORMÉMENT AUX EXIGENCES SUSMENTIONNÉES, Y COMPRIS CELLE DE LIMITER LA DIVULGATION À CE QUI EST STRICTEMENT NÉCESSAIRE AUX FINS AUTORISÉES, CELLE DE LA CONSIGNER ET CELLE DE L'EFFECTUER PAR UN MOYEN SÉCURISÉ.**

REQUÉRANT	DIVULGATION AUTORISÉE³	AUTORITÉ LÉGISLATIVE
Comité d'enquête en vertu de la Loi sur les médecins	Un témoin peut divulguer des renseignements personnels à un comité d'enquête si celui-ci lui a fait parvenir un avis en bonne et due forme indiquant les documents à produire ⁴ .	Loi sur les médecins, art. 31(1) et (2)
Client	Un client peut obtenir l'accès à ses propres renseignements personnels en vertu de la LAIPVP (à certaines conditions). Le sous-ministre peut divulguer des renseignements sur l'état physique ou mental d'une personne à un médecin ou à un autre spécialiste pour obtenir son avis sur le fait que leur divulgation risquerait vraisemblablement ou non de créer un danger imminent et sérieux pour la	LAIPVP, art. 5 Règlement sur l'accès à l'information et la protection de la vie privée, art. 4

² Excepté un avocat du ministère de la Justice, conformément à l'article 48, paragraphes c) et l), de la LAIPVP.

³ N.B. : L'autorité législative de divulguer des renseignements personnels n'est présentée dans le présent tableau que relativement à un contexte de soins de santé; d'autres autorisations concernant les renseignements personnels pourraient être prévues en vertu des mêmes lois dans d'autres contextes.

⁴ La Loi sur les médecins n'autorise pas la divulgation de renseignements personnels d'une personne sans son consentement, sauf dans le cadre d'une enquête en vertu des paragraphes 31(1) et (2).

REQUÉRANT	DIVULGATION AUTORISÉE ³	AUTORITÉ LÉGISLATIVE
	sécurité ou l'état physique ou mental de la personne.	
Coroner	En cas de décès à déclaration obligatoire, le Ministère peut divulguer au coroner les renseignements personnels utiles à son enquête sur réception de son mandat pour prendre possession du corps.	Loi sur les coroners, art. 9(1)
Tutrice ou tuteur/intervenante ou intervenant de la protection de l'enfance	Le Ministère peut divulguer des renseignements personnels à la tutrice ou au tuteur d'un client sur preuve de son ordonnance de tutelle, l'ordonnance devant indiquer les droits précis de la tutrice ou du tuteur à cet égard ainsi que la durée de la tutelle.	Loi sur la tutelle, art. 11(2)
	Des renseignements personnels peuvent être divulgués à une intervenante ou un intervenant de protection de l'enfance si le client est sous la tutelle temporaire ou permanente du directeur des services à l'enfance et à la famille. Une ordonnance accordant la garde permanente ou temporaire du client doit être fournie.	Règlement sur les normes dans les hôpitaux, art. 74(1)g)
	Si un client ayant été appréhendé n'est visé par aucune ordonnance, des renseignements personnels peuvent être divulgués à une intervenante ou un intervenant de la protection de l'enfance dans la seule mesure requise par les soins et le traitement prodigués à ce moment.	Loi sur les services à l'enfance et à la famille, art. 35
Services de santé assurés	Le Ministère peut divulguer des renseignements personnels aux services de santé assurés pour répondre à des besoins administratifs, dont la facturation.	LAIPVP, art. 48a)
Fournisseurs de soins de santé du cercle de soins extérieurs au GN	Le Ministère peut divulguer des renseignements personnels relatifs à la prestation de soins aux fournisseurs de soins de santé hors territoire faisant partie du cercle de soins.	LAIPVP, art. 48a)
Commissaire à l'information et à la vie privée du Nunavut	Le Ministère peut divulguer à la commissaire à l'information et à la vie	LAIPVP, art. 48i)

REQUÉRANT	DIVULGATION AUTORISÉE ³	AUTORITÉ LÉGISLATIVE
	privée du Nunavut les renseignements personnels nécessaires à l'exercice de ses fonctions.	
Médecin-hygiéniste	Sur demande écrite, le Ministère peut divulguer des renseignements personnels à un médecin-hygiéniste.	Règlement sur les normes dans les hôpitaux, art. 74(1)b)
Plus proche parent	Il est permis de divulguer des renseignements personnels pour aviser le plus proche parent d'une personne que celle-ci est blessée, malade ou décédée. Toutefois, la nature de la blessure ou de la maladie ne peut pas être divulguée.	LAIPVP, art. 48r)
Registraire des registres de maladies	Le Ministère peut divulguer des renseignements personnels, dans une forme approuvée par le registraire, lorsqu'un professionnel de la santé examine, diagnostique ou traite une personne pour une maladie à déclaration obligatoire, ou effectue ou fait effectuer sur elle un test à déclaration obligatoire. La forme prescrite doit limiter la nature des renseignements à communiquer à ceux qui sont autorisés par la Loi sur les registres des maladies.	Loi sur les registres des maladies, art. 3 et 5
Chercheurs	Des renseignements personnels peuvent être divulgués à des fins de recherche dans la mesure autorisée par la LAIPVP et approuvée par le Comité de la recherche du GN et le sous-ministre de la Santé, dans les limites permises par la LAIPVP.	LAIPVP, art. 49d) et Règlement sur l'accès à l'information et la protection de la vie privée, art. 8

REQUÉRANT	DIVULGATION AUTORISÉE ³	AUTORITÉ LÉGISLATIVE
Subrogé	<p>Le subrogé d'un client a le droit d'obtenir tous les renseignements qui lui sont nécessaires pour donner son consentement libre et éclairé au nom de ce dernier, y compris les renseignements au sujet du traitement proposé.</p> <p>Si le client est mentalement incapable, le subrogé a le droit d'examiner le dossier médical du client et d'en faire des copies.</p> <p>Si le client est mentalement capable, une personne qui lui a été subrogée lors d'une incapacité antérieure a le droit d'examiner les parties du dossier médical du client concernant des décisions qu'elle a prises au nom du subrogé et d'en faire des copies.</p>	Loi sur la santé mentale, art. 19.4 et 49.4
En vertu d'un subpœna, d'un mandat ou d'une ordonnance	Il est permis de divulguer des renseignements personnels en vertu d'un subpœna, d'un mandat ou d'une ordonnance de tribunal autorisant la divulgation de renseignements précis; ladite divulgation doit se limiter à ce que vise le subpœna, le mandat ou l'ordonnance.	LAIPVP, art. 48n)
Anciens Combattants Canada	Le Ministère peut faire droit à une demande écrite d'Anciens Combattants visant à obtenir des renseignements personnels d'un client qui est ou a été membre des forces armées, navales ou aériennes du Canada ou qui est par ailleurs admissible aux services de ce ministère.	Règlement sur les normes dans les hôpitaux, art. 74i)
Statistiques de l'état civil	Les renseignements personnels nécessaires au recensement des naissances, des mortinaissances et des décès peuvent être divulgués au registraire général.	Loi sur les statistiques de l'état civil, art. 2, 12 et 19
Commission de la sécurité au travail et de l'indemnisation des travailleurs	Sur réception d'une lettre type dument remplie de la Commission de la sécurité au travail et de l'indemnisation des travailleurs, le Ministère peut divulguer tout renseignement personnel nécessaire	Loi sur l'indemnisation des travailleurs, art. 30 Règlement sur les normes dans les hôpitaux, art. 74(1)h)

REQUÉRANT	DIVULGATION AUTORISÉE ³	AUTORITÉ LÉGISLATIVE
	<p>à cette dernière pour motiver une décision quant à une demande d'indemnisation.</p> <p>Un fournisseur de soins de santé qui examine ou traite un travailleur dans le cadre de la Loi sur l'indemnisation des travailleurs peut soumettre à la Commission un rapport contenant des renseignements personnels.</p>	<p>Loi sur l'indemnisation des travailleurs, art. 25(1)</p>
Divers	<p>Des renseignements personnels peuvent être divulgués en vertu d'une loi du Nunavut ou du Canada⁵.</p> <p>Des renseignements personnels peuvent être divulgués si la protection d'une personne, y compris celle de sa santé mentale ou physique, l'exige.</p> <p>Des renseignements personnels peuvent être divulgués pour des motifs d'intérêt public, ou si la personne qu'ils concernent en tirerait un avantage certain, moyennant autorisation du sous-ministre.</p> <p>Des renseignements personnels peuvent être divulgués pour l'examen formel d'un programme gouvernemental, si l'examen est sanctionné par une loi, un règlement ou une politique publique.</p> <p>Des renseignements personnels peuvent être divulgués à des fins de vérification au vérificateur général ou au ministère des Finances.</p>	<p>LAIPVP, art. 48q)</p> <p>LAIPVP, art. 48s)</p> <p>Règlement sur l'accès à l'information et la protection de la vie privée, art. 6</p> <p>LAIPVP, art. 48j) Règlement sur l'accès à l'information et la protection de la vie privée, art. 7</p>

8. ADMINISTRATION

La présente directive sera examinée par le sous-ministre de la Santé chaque année ou dès la tenue d'une enquête sur une atteinte à la confidentialité visant une collecte, une utilisation ou une divulgation de renseignements personnels autorisée, ou la formulation d'une conclusion négative dans le cadre d'une analyse ou d'une vérification des facteurs relatifs à la vie privée. Le rapport de cet examen sera déposé auprès du ministre de la


⁵ Notamment en vertu des pouvoirs de vérification et d'enquête conférés par une loi du Nunavut, par exemple la Loi sur la profession de sage-femme, articles 26 (nomination des vérificateurs) et 34 (enquête).

Santé.

9. AUTORISATION

Le sous-ministre de la Santé,

Date

 Ministère de la Santé Gouvernement du Nunavut	DIRECTIVE DU MINISTÈRE DE LA SANTÉ		
	DIRECTIVE SUR LA SÉCURITÉ ET LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS LES DSEi		
TITRE :		SECTION :	NUMÉRO DE POLITIQUE :
Directive sur le contrôle d'accès aux systèmes de cybersanté			
DATE D'ENTRÉE EN VIGUEUR :	DATE DE RÉVISION :	REPLACE LE NUMÉRO :	NOMBRE DE PAGES :
			4
APPLICABLE À :			
Tous les employés, fournisseurs et agents du GN qui utilisent les systèmes de dossiers de santé électroniques.			

1. PRÉAMBULE

La présente directive a pour but de guider les employés, fournisseurs et agents du gouvernement du Nunavut (GN) sur les questions liées à la gestion de l'accès aux systèmes de cybersanté, incluant les dossiers de santé électroniques interopérables (DSEi).

Le ministère de la Santé est assujéti à la Loi sur l'accès à l'information et à la protection de la vie privée (AIPVP), une loi qui a été édictée pour rendre les organismes publics redevables à la population par rapport au traitement des informations et à la protection de la vie privée. Les renseignements personnels sur la santé sont compris dans la définition des renseignements personnels de l'AIPVP.

L'article 42 de l'AIPVP requiert que le ministère de la Santé protège les renseignements personnels « en prenant les mesures de sécurité voulues contre des risques tels que l'accès, la collecte, l'usage, la divulgation et le retrait non autorisés. »

Les clients font confiance au GN et s'attendent à ce que celui-ci protège la confidentialité, l'intégrité et le caractère privé de leurs renseignements personnels. Il est essentiel de satisfaire ces attentes afin de promouvoir la sécurité des clients et gagner leur confiance et leur loyauté.

2. PRINCIPES

1. Le ministère de la Santé contrôle l'accès aux systèmes de cybersanté conformément aux principes suivants :

- a. la priorité de consolider les services publics en développant les infrastructures en cybersanté qui améliorent et rendent plus efficiente et efficace la gestion des renseignements personnels;
- b. l'*Inuit Qaujimagatuqangit* qui consiste en *Piliriqatigiinniq* (travailler ensemble vers un but commun), *Inuuqatigiitsiarniq* (respecter les autres, les relations et prendre soin des gens), *Tunnganarniq* (nourrir une bonne attitude en étant ouvert, accueillant et inclusif) et *Pilimmaksarniq* (acquérir des compétences par la pratique, l'effort et l'action);
- c. le GN, incluant le ministère de la Santé, a l'obligation légale de protéger les renseignements et dossiers personnels qu'il détient en prenant les mesures de sécurité voulues contre des risques tels que l'accès, la collecte, l'usage, la divulgation et le retrait non autorisés de ces renseignements;

- d. l'accès aux systèmes de cybersanté est accordé selon les rôles;
- e. le ministère de la Santé définit les rôles des utilisateurs en collaboration avec les parties prenantes;
- f. les rôles sont attribués aux utilisateurs des systèmes de cybersanté par leur supérieur;
- g. l'accès aux systèmes de cybersanté et à leurs ressources est accordé en fonction du rôle et des besoins d'information de l'utilisateur;
- h. toutes les activités des utilisateurs, incluant l'accès aux systèmes de cybersanté, peuvent être surveillées et auditées par le GN.

3. PORTÉE ET APPLICATION

La présente directive sur le contrôle d'accès aux systèmes de cybersanté s'applique à :

- 1. tous les utilisateurs, incluant les employés, contractuels et agents du GN, ainsi que tous les vendeurs et fournisseurs de produits et services au GN qui accèdent aux systèmes de cybersanté, les utilisent, les opèrent ou les entretiennent;
- 2. l'accès physique et logique aux systèmes de cybersanté et aux ressources des systèmes connexes;
- 3. tous les systèmes de cybersanté et aux ressources des systèmes connexes, incluant :
 - a. les données confidentielles :
 - i. renseignements personnels;
 - ii. journaux d'audit des systèmes;
 - iii. données administratives du système et de la sécurité (par ex. configurations de la sécurité technique, informations de mots de passe et d'authentification);
 - b. le matériel comme les appareils mobiles et l'équipement de réseautique;
 - c. les logiciels;
 - d. les ressources en communication et réseautique.

4. RÔLES ET RESPONSABILITÉS

- 1. Le ministère de la Santé a la responsabilité première de déterminer le niveau de confidentialité des ressources des systèmes de cybersanté, incluant les renseignements personnels. Les renseignements qui sont traités et stockés dans les systèmes de cybersanté sont classés confidentiels.
- 2. Le ministère des Services communautaires et gouvernementaux conserve la responsabilité de contrôler l'accès aux environnements techniques et aux infrastructures qui abritent les systèmes de cybersanté.
- 3. Les mesures de contrôle d'accès sont appliquées en fonction du niveau de confidentialité des ressources et du risque de violation, mesuré par une évaluation des menaces et des risques (EMR).

5. DÉTERMINATION DES PRIVILÈGES D'ACCÈS

- 1. L'accès aux ressources du système est déterminé en fonction du rôle, du poste, de la fonction et du groupe de travail et se limite à ce qui est strictement nécessaire.
- 2. La Division des renseignements sur la santé de la population (DRSP) élabore un tableau des contrôles d'accès dans lequel les rôles des utilisateurs et les privilèges d'accès sont définis. Les rôles et les privilèges d'accès s'y rattachant sont déterminés en consultation avec les ministères et groupes utilisateurs.
- 3. La DRSP peut définir les groupes de travail et donner aux utilisateurs individuels l'accès aux renseignements personnels et autres ressources de cybersanté en fonction de leur groupe de travail.
- 4. La DRSP peut mettre en service une fonctionnalité dans le système de cybersanté qui

connecte les utilisateurs aux dossiers de leurs clients. Cela donne à l'utilisateur le pouvoir discrétionnaire d'accorder un droit d'accès à un autre utilisateur enregistré.

6. ATTRIBUTION DES PRIVILÈGES D'ACCÈS

1. Le gestionnaire ou superviseur de l'utilisateur qui reçoit une autorisation d'accès lui attribue un rôle ou un groupe avec les privilèges d'accès correspondants. Un même utilisateur peut avoir plusieurs rôles.
2. Le gestionnaire ou superviseur de l'utilisateur qui reçoit une autorisation d'accès doit confirmer que celui-ci a reçu la formation requise, a signé une entente de confidentialité et a lu et compris la *politique du GN en matière d'atteinte à la vie privée (Privacy Breach and Incident Policy)*, la *politique sur l'utilisation acceptable des courriers électroniques et de l'Internet (Acceptable E-Mail and Internet Usage Policy)* et la directive sur la sécurité et la protection des renseignements personnels dans les DSEi.

7. IDENTIFICATION ET INSCRIPTION DES UTILISATEURS

1. La DRSP va mettre en place des procédures d'inscription pour les utilisateurs de manière à s'assurer que :
 - a. le niveau d'identification requis par l'utilisateur correspond au niveau de protection requis pour garantir la confidentialité des renseignements personnels et des ressources du système en tenant compte des fonctions qui deviendront accessibles à l'utilisateur;
 - b. chaque utilisateur potentiel a un lien légitime avec l'organisation;
 - c. chaque utilisateur potentiel a un besoin légitime d'accéder aux renseignements personnels et autres ressources confidentielles du système.
2. L'utilisateur autorisé reçoit une identification qui, en combinaison avec d'autres identifiants (par ex. mots de passe, jetons de sécurité, identifiants de lieu ou d'établissement), permet de l'identifier de manière précise;
3. La DRSP mettra en service une fonctionnalité dans les systèmes de cybersanté qui rend compte pour chaque utilisateur des :
 - a. dossiers qu'il peut accéder;
 - b. parties de dossiers qu'il peut accéder;
 - c. privilèges (par ex. visualisation, ajout, suppression, modification) qu'il possède pour chacun de ces dossiers.
4. Les privilèges d'accès de l'utilisateur sont révisés et renouvelés annuellement, et ses informations sont revues et mises à jour si nécessaire par la même occasion.
5. Les privilèges d'accès de l'utilisateur sont retirés aussitôt qu'ils ne sont plus requis, par exemple lors d'une cessation d'emploi ou d'un changement de fonction ou de rôle. La DRSP élaborera des procédures de révocation des privilèges d'accès aux systèmes de cybersanté.
6. La séparation doit être claire entre les tâches du personnel qui administre le système et accorde l'accès aux informations et ressources confidentielles, celles des utilisateurs et de leurs superviseurs et celles des gestionnaires qui accèdent au système et utilisent ses ressources.

8. JOURNAUX D'AUDIT ET SURVEILLANCE DES ACCÈS AU SYSTÈME

1. La DRSP mettra en service une fonctionnalité permettant la production de journaux et de rapports d'audit dans les systèmes de cybersanté de manière à ce que chaque consultation, ajout, modification, suppression ou archivage de renseignements personnels effectué par l'utilisateur soit consigné dans un journal d'audit.
2. La DRSP mettra en service une fonctionnalité permettant la production de journaux et de rapports d'audit servant à rapporter chaque accès aux renseignements personnels

des clients dans les systèmes de cybersanté.

3. L'accès aux journaux et outils d'audit sera protégé par la DRSP afin de prévenir les utilisations abusives et éviter que la sécurité soit compromise.
4. La DRSP mettra en place un programme de surveillance et d'audit pour détecter les accès non autorisés aux ressources de cybersanté, incluant aux renseignements personnels, et prendre les mesures appropriées lorsqu'il y a présumée violation de la sécurité ou de la vie privée.

9. ACCÈS DE L'UTILISATEUR AUX SYSTÈMES DE CYBERSANTÉ

1. L'utilisateur ne peut se servir que d'un seul rôle à la fois pour accéder aux services et aux systèmes de cybersanté (l'utilisateur qui a été inscrit avec plusieurs rôles ne se chevauchant pas doit en choisir un seul pour ouvrir une session dans le système de cybersanté).
2. Lorsque requis, l'authentification peut exiger des certificats numériques, jetons de sécurité ou données biométriques pour donner accès à des ressources confidentielles du système.
3. L'accès physique ou logique à des postes de travail non surveillés est limité et des mesures seront mises en place afin de s'assurer qu'une personne non autorisée ne puisse pas utiliser un poste de travail lorsque le système de cybersanté est ouvert.

10. CONTRÔLE DE L'ACCÈS AUX ENVIRONNEMENTS TECHNIQUES

1. Le ministère des Services communautaires et gouvernementaux (SCG) s'assure que toutes les connexions distantes aux services et applications sont authentifiées, incluant les connexions par Internet.
2. Les SCG contrôlent l'accès aux diagnostics et services de gestion des réseaux des systèmes de cybersanté, incluant l'accès aux ports et services de diagnostic des réseaux qui hébergent ces composantes.
3. Les SCG contrôlent l'accès aux programmes utilitaires des systèmes de cybersanté et restreignent leur utilisation.

11. ADMINISTRATION DE LA PRÉSENTE DIRECTIVE

La présente directive est revue chaque année par les sous-ministres de la Santé et des Services communautaires et gouvernementaux ou dès qu'une enquête est déclenchée sur une présumée violation de la sécurité relative au contrôle d'accès ou encore lorsque l'évaluation des menaces et des risques ou l'audit de sécurité portant sur le contrôle d'accès mène à des résultats négatifs. Le rapport de révision est remis aux ministres de la Santé et des Services communautaires et gouvernementaux.

12. AUTORISATION

Sous-ministre
Ministère de la Santé

Date

Sous-ministre
Ministère des Services communautaires
et gouvernementaux

Date