DESCRIPTION EN LANGAGE CLAIR DES SERVICES ET DE LA SÉCURITÉ DU RÉSEAU DU NORD-EST DE L'ONTARIO (NEON)

La *Loi de 2004 sur la protection des renseignements personnels sur la santé* (LPRPS, 2004) définit un « fournisseur d'un réseau d'information sur la santé » (FRIS) comme une personne ou un organisme qui fournit des services à deux dépositaires de renseignements sur la santé (DRS) ou plus principalement dans le but de leur permettre d'utiliser des moyens électroniques pour se divulguer entre eux des renseignements personnels sur la santé (RPS). En tant que FRIS, Horizon Santé-Nord (HSN) évalue les menaces, risques et impacts associés au système d'information partagé et s'emploie à protéger les RPS et à respecter ses obligations en matière de sécurité et de protection de la vie privée.

Description

Le système d'information partagé de NEON est le système de gestion de l'information sur la santé de Meditech dont HSN a fait l'acquisition et qui comprend le logiciel, l'ordinateur central, les réseaux et les interfaces.

Résumé des mesures de sécurité et de protection de la vie privée

Chaque organisme partenaire a la responsabilité de prendre des mesures raisonnables pour empêcher l'utilisation et la divulgation non autorisées de renseignements confidentiels. Les DRS participants ont l'obligation, aux termes de la loi ontarienne sur la confidentialité des RPS, soit la *Loi de 2004 sur la protection des renseignements personnels sur la santé* (LPRPS), de prévoir les mesures de protection suivantes :

- ***Hébergement sécurisé***
  Le système d'information partagé de NEON est hébergé dans un environnement sécurisé et est protégé par des mesures de sécurité efficaces mises en place conformément aux meilleures pratiques de l'industrie
- ***Autorisation***
  L'identité des utilisateurs est vérifiée avant que l'accès au système d'information partagé de NEON ne leur soit accordé
  L'accès au système d'information partagé de NEON par un utilisateur doit être autorisé par l'administration de l'organisme partenaire conformément à la politique de NEON
- ***Authentification***
  Tous les utilisateurs sont authentifiés par le biais d'un mécanisme d'authentification avant d'avoir accès au système d'information partagé de NEON
- ***Sécurité des données***
  Les données du système d'information partagé de NEON ne peuvent être modifiées par un utilisateur à moins que celui-ci n'ait obtenu auparavant l'autorisation de le faire
  Des politiques et procédures sur la conservation et l'élimination des données ont été mises en place pour assurer la disponibilité et la confidentialité des données du système d'information partagé de NEON
- ***Journalisation***
  Les événements liés à la sécurité et à protection de la vie privée comme l'accès à des RPS et les actions administratives sont enregistrés
  Des journaux de vérification sont examinés par chaque organisme participant afin de détecter toute activité suspecte ou violation à la vie privée ou à la sécurité potentielle
- ***Évaluations de la sécurité***
  Des évaluations des menaces et des risques (EMR), ainsi que des évaluations de l'impact sur la vie privée (EIVP) concernant les services fournis sont réalisées afin de déterminer les besoins d'amélioration et d'atténuation des risques

- ***Vie privée***

  Chaque participant et l'organisme qui offre des services de FRIS ont mis en place et adopté des pratiques en matière de collecte, d'utilisation et de divulgation de RPS conformes à la LPRPS et à ses règlements

  Un processus de gestion des incidents est en place pour permettre aux organismes participants de détecter les incidents, de faire enquête à leur sujet et de les gérer de manière collaborative

  Un processus de soutien à la protection de la vie privée est en place pour gérer les demandes des clients/patients relatives à l'accès aux RPS du système d'information partagé de NEON et à leur correction pour garantir la conformité de l'organisme participant aux mesures de protection de la vie privée

Conclusion

Les organismes participants qui utilisent le système d'information partagé de NEON respectent les dispositions de la LPRPS et les normes pertinentes de l'industrie. Ils ont mis en place un ensemble de mesures de sécurité administratives, physiques et techniques pour protéger les RPS. De plus, ces organismes ont adopté des politiques et procédures pour s'assurer que leurs employés et les autres utilisateurs autorisés du système d'information partagé de NEON comprennent leurs obligations relativement au système et à la protection des RPS.