Description en langage clair du réseau et de la sécurité du service d'intégration des cabinets médicaux (icm)

La description suivante du service d'intégration des cabinets médicaux (ICM) sert à souligner les mesures de sécurité et de protection de la vie privée qui s'y appliquent.

Description du service d'intégration des cabinets médicaux

Le service d'ICM est une méthode de distribution des rapports au moyen d'une interface électronique gérée par Horizon Santé-Nord. À l'aide du service d'ICM, les fournisseurs de soins primaires participants reçoivent les rapports et les résultats des patients envoyés par les établissements de soins directement dans leur système de dossiers médicaux électroniques (DME). Le service d'ICM utilise un protocole de transfert de fichiers sécurisé, sur Internet, pour mettre cette information à la disposition des cabinets des médecins.

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

De nombreuses procédures de sécurité sont intégrées dans le service d'ICM pour protéger les renseignements personnels sur la santé (RPS). Les dépositaires de renseignements sur la santé (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 service d'ICM 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 service d'ICM ne leur soit accordé
- L'accès au service d'ICM par un utilisateur doit être autorisé par l'administration de son établissement de soins ou de son cabinet de soins primaires conformément au processus de gestion des comptes utilisateurs

Authentification

- Tous les utilisateurs sont authentifiés par le biais d'un mécanisme d'authentification sophistiqué avant d'avoir accès au service d'ICM

Sécurité des données

- Les données du service d'ICM ne peuvent être modifiées par aucun utilisateur
- 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 service d'ICM

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 mis à la disposition du responsable de la protection de la vie privée de l'organisme participant afin que cette personne puisse les examiner périodiquement pour détecter toute activité suspecte ou violation à la vie privée ou à la sécurité potentielle

Évaluations de la sécurité

- Une évaluation des menaces et des risques (EMR) et une évaluation de l'impact sur la vie privée (EIVP) ont été réalisées afin de déceler toute vulnérabilité ou faille en matière de sécurité et de protection de la vie privée
- Un test d'intrusion a été réalisé pour prévenir tout accès et changement non autorisés au service d'ICM et à ses données

Vie privée

- Chaque participant et l'organisme qui offre des services de fournisseur d'un réseau d'information sur la santé (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 du consentement est en place pour gérer et appliquer le consentement des clients/patients parmi les organismes participants
- 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 service d'ICM et à leur correction et pour garantir la conformité de l'organisme participant aux mesures de protection de la vie privée

Conclusion

Participating organizations that use the POI Service comply with the provisions of PHIPA and relevant industry standards. They use a variety of administrative, physical and technical safeguards to protect PHI. In addition, participating organizations have policies and procedures in place to ensure that their employees and other authorized users of the POI Service understand their obligations with respect to the system and protection of PHI.