Plain Language Description of Network Services and Security for the Northeast Ontario Network (NEON)

The Personal Health Information and Protection Act (PHIPA, 2004) defines a Health Information Network Provider (HINP) as a person or organization which provides services to two or more Health Information Custodians (HICs) primarily to enable the custodians to use electronic means to disclose personal health information (PHI) to one another. As a HINP, Health Sciences North (HSN) assesses the threats, risks and impacts associated with the shared system and works to safeguard the PHI and meet its obligations related to privacy and security.

Description

The NEON shared information system is the health information management system purchased by HSN from Meditech and includes the Meditech Software, Mainframe, Networks and Interfaces.

Summary of Privacy and Security Safeguards

Each partner organization is responsible to take reasonable steps to prevent any unauthorized use or disclosure of Confidential Information. Participating HICs are obligated under the Ontario health information privacy legislation, the Personal Health Information Protection Act, 2004 (PHIPA) to provide the following safeguards:

Secure Hosting

- The NEON Shared Information System is hosted in a secure environment with effective security safeguards in place that are in compliance with industry best practices

Authorization

- Users' identities are verified before they are granted access to the NEON Shared Information System
- Users' access to the NEON Shared Information System must be authorized by the administration of the partner organization in accordance with NEON policy

Authentication

- All users are authenticated through an enhanced authentication mechanism prior to accessing the NEON Shared Information System

Data Security

- NEON Shared Information System data cannot be changed or modified by any users unless they have received prior authorization
- Data retention and disposal policies and procedures are in place to ensure the availability and confidentiality of NEON Shared Information System data

Logging

- Privacy and security related events and activities such as access to PHI and administrative actions are logged

- Audit logs are reviewed by each participating organization to detect suspicious activities or potential Privacy/Security Breaches

Security Assessment

- Perform Threat Risk Assessment (TRA) and Privacy Impact Assessment (PIA) of services provided to identify improvements and mitigate risks

Privacy

- Each participant and the organization that provide HINP services have implemented and followed information practices that comply with PHIPA and its regulations regarding the collection, use and disclosure of PHI
- An incident management process is in place to detect, investigate and manage incidents collaboratively among participating organizations
- A client privacy support process is in place to manage Clients/Patients' requests to access and/or correct their PHI in the NEON Shared Information System, and to challenge the privacy compliance of the participating organization

Conclusion

Participating organizations that use the NEON Shared Information System 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 NEON Shared Information System understand their obligations with respect to the system and protection of PHI.