Plain Language Description of Network Services and Security for the Physician Office Integration Service

The following description of the Physician Office Integration (POI) Service has been created to highlight privacy and security safeguards within the POI Service.

Description of the Physician Office Integration Service

The POI Service is a report distribution option that occurs via an electronic interface hosted by Health Sciences North. Using the POI Service, participating primary care providers receive patient reports/results from health care facilities into their Electronic Medical Record (EMR) systems. The POI Service uses a secure file transfer protocol over the internet to make this information available to physicians' offices.

Summary of Privacy and Security Safeguards

There are numerous controls built into the POI Service to protect PHI. Participating Health Information Custodians (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 POI Service 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 POI Service
- Users' access to the POI Service must be authorized by the administration of their health care facility or primary care office in accordance with the established User Account Management Process

Authentication

- All users are authenticated through an enhanced authentication mechanism prior to accessing the POI Service

Data Security

- POI data can not be changed or modified by any users
- Data retention and disposal policies and procedures are in place to ensure the availability and confidentiality of POI data

Logging

- All privacy and security related events and activities such as access to PHI and administrative actions are logged
- Audit logs are made available to be reviewed by a participating organization's Privacy Lead on a regular basis to detect suspicious activities or potential Privacy/Security Breaches

Security Assessment

- A Threat Risk Assessment (TRA) and Privacy Impact Assessment (PIA) were conducted to identify privacy and security gaps and deficiencies.
- Penetration testing has been performed to prevent any unauthorized access and modification to the POI Service and its data

Privacy

- Each participant and the organization that provide Health Information Network Provider services have implemented and followed information practices that comply with PHIPA and its regulations regarding the collection, use and disclosure of PHI
- A consent management process is in place to manage and enforce Client/Patient's consent among participating organizations
- 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 POI Service, and to challenge the privacy compliance of the participating HSP

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.