Plain Language Description of Network Services and Security for the Integrated Assessment Record

The following description of the Integrated Assessment Record (IAR) has been created to highlight privacy and security safeguards within the IAR system.

Description of the Integrated Assessment Record System

The IAR is a web-based tool for authorized Participants who are involved in a Client/Patient's care, to access Client/Patient assessment information such as the Ontario Common Assessment of Need (OCAN) and the Resident Assessment Instrument for Mental Health (RAI-MH). The IAR offers a secure and accurate method of viewing Client/Patient's Personal Health Information (PHI) as part of the client assessment process. Regardless of where a person receives service, Participants will have the ability to view a snapshot or a subset of the Client/Patient's most recent assessment information while maintaining access to the other full assessments if required.

Summary of Privacy and Security Safeguards

There are numerous controls built into the system 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 IAR solution 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 IAR
- Users' access to IAR must be authorized by the administration of their Health Service Provider (HSP) organization in accordance with the established User Account Management Process

Authentication

- All users are authenticated through an enhanced authentication mechanism prior to accessing the IAR
- Strong password policy is enforced in the IAR system solution

Data Security

- IAR data is encrypted in storage and in transit
- IAR 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 IAR data

Logging

- All privacy and security related events and activities such as access to PHI and administrative actions are logged
- Audit logs are reviewed by Participating organization's privacy officer 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, which were mitigated appropriately to ensure compliance
- Penetration testing has been performed to prevent any unauthorized access and modification to the IAR and the data

Privacy

- Each Participant and the organizations that provide Health Information Network Provider (HINP) services have implemented and followed information practices that comply with PHIPA and its regulations regarding the collection, use and disclosure of PHI
- An integrated consent management process is in place to manage and enforce Client/Patient's consent among participating organizations
- An integrated incident management process is in place to detect, investigate and manage incidents collaboratively among participating organizations
- An integrated client privacy support process is in place to manage Clients/Patients' requests to access and/or correct their PHI in the IAR, and to challenge the privacy compliance of the participating HSP

Conclusion

Participating organizations that use the IAR 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 system understand their obligations with respect to the system and protection of PHI.