SAFEGUARDS REGARDING CONFIDENTIALITY AND SECURITY OF THE INTEGRATED ASSESSMENT RECORD

Administrative

- An individual(s) has been designated as being responsible for privacy and security compliance
- An organizational governance framework for privacy, confidentiality, and security is in place which includes clearly defined roles and responsibilities for privacy and security
- Organizational policies and procedures for privacy and security management have been developed, implemented and are monitored and enforced. A mechanism is in place for reviewing and updating the policies and procedures
- Only "authorized" staff may have access to and use of the Integrated Assessment Record (IAR) on a "need-to-know" basis (i.e. when required to perform their duties)
- Nondisclosure or confidentiality agreements are in place for all employees, staff, volunteers and contractors which contain appropriate sanctions for breach of privacy, confidentiality, or security, up to and including dismissal or termination of the agreement, whatever the case may be
- A Threat Risk Assessment (TRA) and Privacy Impact Assessment (PIA) have been conducted for the IAR
- Mandatory and ongoing privacy, confidentiality, and security training is conducted for all employees, staff, volunteers and contractors working with the IAR
- A "Privacy/Security Breach" protocol with respect to the privacy and security of the IAR system and data has been developed and implemented
- 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 personal health information in the IAR, and to challenge the privacy compliance of the participating Health Service Provider
- Acceptable business recovery plans, including disaster recovery and data backup are in place
- Signed agreements have been in place with any third parties who assist in providing Health Information Network Provider (HINP) services to the Health Information Custodians pursuant to this Agreement, which require such third parties to implement appropriate privacy and security safeguards in providing such services

Technical

- Strong access control mechanisms, including authorization and authentication measures (such as computer password protection and unique log-on identification) have been implemented to ensure that only authorized personnel can access the IAR
- IAR data is encrypted in storage and in transit
- IAR data cannot be changed or modified by any users
- Remote electronic access to the IAR hosting environment is prohibited except where required for delivery of support services by those individuals executing these responsibilities on behalf of the HINP and who have been assigned the appropriate access rights by the HINP
- Virus-checking programs have been implemented
- Detailed real-time audit trails have been implemented to record the user name, timestamp, and nature of data access

Physical

- Computers and files that hold the IAR are housed in secure settings in rooms protected by such methods as combination lock doors or smart card door entry, with paper files stored in locked storage cabinets
- Employees and staff have been provided with photo identification or coded swipe cards
- Contractors and volunteers are required to have appropriate photo identification or coded swipe cards limiting their access to those parts of the premises which are required in order for them to provide their services
- Visitors to the data centre are screened and supervised
- Alarm systems are in place
- The number of locations in which the IAR is stored has been minimized and specified in advance
- The architectural space of the HINP precludes public access to areas where the IAR is held
- Routine surveillance of premises is conducted
- Fire suppression systems are in place to protect the IAR from fire hazards