Safeguards regarding confidentiality and security of the MEDITECH system

Waypoint
CENTRE for MENTAL HEALTH CARE
CENTRE de SOINS de SANTÉ MENTALE

Your personal health information is kept confidential and secure and is not disclosed to anyone outside Waypoint, Ontario Shores or The Royal without your consent, unless disclosure is permitted or required by law. As Health Information Custodians and Waypoint as the Health Information Network Provider, we take steps to ensure that everyone who performs services for us protects your privacy and only uses your personal health information for the purposes you have consented to.

To protect your personal health information, we take:

1. **Administrative Measures**

- 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 roles and responsibilities for privacy, security, oversight and decision-making;
- 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 policies and procedures;
- Only "authorized" staff may have access to and use the MEDITECH system on a "need-to-know" basis i.e. when required to perform their duties;
- Nondisclosure or confidentiality agreements are in place for all employees, medical staff, consultants, contractors, volunteers, students and affiliates 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 Privacy Impact Assessment (PIA) and a threat risk assessment (TRA) have been conducted for the MEDITECH system;
- Mandatory and ongoing privacy, confidentiality and security training is conducted for all employees, medical staff, volunteers working with MEDITECH and contractors who may need to access personal health information or personal information in the provision of their services;
- A "Privacy and Security Breach" protocol with respect to identifying and managing the unauthorized collection, use and disclosure of personal health information and the confidentiality, integrity and availability of the MEDITECH system and data that has been developed and implemented. An integrated incident management process is in place to detect,

investigate and manage incidents collaboratively among Participating Organizations;

- A consent management process is in place to manage and enforce a Patient's wishes to limit access to personal health information among Participating Organizations;
- An integrated patient privacy support process is in place to manage patients' requests to access and/or correct their personal health information in the MEDITECH system and to challenge the privacy compliance of the participating Health Service Provider;
- Acceptable business recovery plans, including, disaster recovery and data back-up are in place; and
- 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 (HICs) pursuant to this Agreement which requires such third parties to implement appropriate privacy and security safeguards in providing such services.

2. Technical Measures

- Strong access control mechanisms, including, authorization and authentication measures i.e. computer password protection and unique log-on identification have been implemented to ensure that only authorized personnel can access the MEDITECH system;
- MEDITECH data can only be changed or modified by users with assigned permissions;
- Remote electronic access to the Meditech 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; and
- Detailed real-time audit trails have been implemented to record the user name, timestamp, and nature of the data access.

3. Physical Measures

- Computers, servers and files that hold the MEDITECH system 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, medical staff, students and volunteers have been provided with photo identifying coded swipe cards;
- Contractors and consultants are provided with contractor or consultant's non-photo identifying cards are escorted on the premises and their access

limited 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.
- The number of locations in which the MEDITECH system is stored has been minimized and specified in advance;
- The architectural space of the HINP precludes public access to areas where the MEDITECH system is being held;
- Routine surveillance of premises is conducted; and
- Fire suppression systems are in place to protect the MEDITECH system from fire hazards.