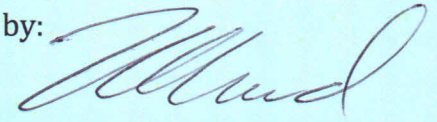
RGP Information Security Policy

Effective Date: October 1, 2016

REGIONAL GERIATRIC PROGRAM OF TORONTO

Better health outcomes for frail seniors

Table of Contents

RGP Information Security Policy	
Effective Date: October 1, 2016	Review Date: August 18,2016
Approved by:  Marlene Awad, Director of Operations	Version: V1.0

1 Purpose

The purpose of this Information Security Policy is to provide guidance to the management, employees and contractors of the Regional Geriatric Program of Toronto (RGP) on matters concerning the management of information security with respect to the RGP Registry System and the business operations of the RGP.

Section 12.(1) of the Personal Health Information Protection Act (PHIPA) requires that *"A health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure the records containing the information are protected against unauthorized copying, modification or disposal."*

Patients, families, caregivers and participating organizations expect and trust that the RGP will protect the confidentiality, integrity and availability of their Personal Health Information (PHI). The RGP is committed to meeting these expectations and to ensuring compliance with PHIPA and security best practices.

2 Abbreviations and Acronyms

IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
PHI	Personal Health Information
PHIPA	Personal Health Information Protection Act
PIA	Privacy Impact Assessment
RGP	Regional Geriatric Program of Toronto

3 Scope and Applicability

This Information Security Policy applies to:

1. All agents (i.e. employees, volunteers, and contractors) of the RGP who have access to PHI or who work in proximity to media containing PHI.
2. All Participating Organizations and their respective agents who may have access to, and use, the RGP Registry System.
3. All RGP information assets including PHI, system administration and security data, hardware, software and communications networks and facilities.
4. All activities associated with the operation of the RGP Registry System and the business operations of the RGP.

4 Principles

1. The RGP shall comply with the *Ontario Personal Health Information Protection Act – 2004* (PHIPA) and its regulations.

2. The RGP adopts *ISO/IEC 27002:2013 – Code of Practice for Information Security Management*, as its guide to developing and deploying its information security program. Security controls will be implemented as required based on an assessment of security risk. This may include controls in the areas of:

    a. Risk Assessment and Treatment
    b. Security Policy
    c. Organization of Information Security
    d. Asset Management
    e. Human Resources Security
    f. Physical and Environment Security
    g. Communications and Operations Management
    h. Access Control
    i. Information Systems Acquisition, Development and Maintenance
    j. Information Security Incident Management
    k. Business Continuity Management
    l. Compliance with Laws, Policies and Standards

5 Roles and Responsibilities

1. The Board of Directors of the RGP is responsible for ensuring that the RGP is in compliance with PHIPA, its regulations and with the security and privacy policies of the RGP.

2. Responsibility for implementing an Information Security Management Program is delegated to the Director of Operations of the RGP. The Director of Operations is responsible for:

a) Developing and maintaining an Information Security Policy.
b) Ensuring that all employees, volunteers and contractors are trained in security procedures and understand their responsibilities for the protection of PHI and critical information systems.
c) Detecting and investigating security and privacy incidents and taking appropriate corrective action.
d) Ensuring that Participating Organizations have understood the responsibilities of managing PHI in their own institutions and have signed Agreements that define the respective privacy and security responsibilities of the RGP and Participating Organizations.

3. The Information Coordinator for the RGP is responsible for:

a) The day-to-day application of reasonable administrative security management measures to protect PHI against unauthorized access, collection, use, disclosure, retention or disposal and to ensure the availability and integrity of PHI.
b) providing guidance and training to RGP staff, volunteers, contractors and Participating Organizations on information security matters associated with the RGP Registry System and RGP operations.
c) Monitoring The RGP Registry System for attacks by internal malicious agents[1] identified through the RGP monitoring and audit program.
d) Developing, testing and maintaining a business continuity plan to ensure minimal disruption to health services in the event of a catastrophic system failure.
e) Detecting, investigating and responding to security incidents.

4. The Technical Analyst for the RGP is responsible for:

a) The implementation of reasonable technical security measures to protect PHI, the RGP Registry System and associated systems and communications networks.
b) Ensuring that necessary safeguards to protect the RGP Registry System against threats identified in Privacy Impact Assessments (PIA), penetration tests and vulnerability assessments are implemented.
c) Identifying, evaluating, and documenting all RGP Registry System assets, including PHI, systems administration and security data, hardware, software and communications facilities and assign levels of sensitivity, criticality and ownership to them.
d) Ensuring that the RGP Registry System is configured and maintained in accordance with security policies, standards and procedures.
e) Monitoring The RGP Registry System for attacks by external malicious agents.[2]

5. All employees, volunteers, and contractors of the RGP are responsible for:

---

[1] Includes the staff of the RGP and participating organizations.
[2] Includes hackers and malicious software (i.e. viruses, spyware, ransomware)

a) Understanding and following all security and privacy policies and procedures established by the RGP.
b) Safeguarding the privacy and confidentiality of PHI collected, used and disclosed in the course of their duties.
c) Acting in a timely and co-operative manner to prevent, detect and respond to security and privacy breaches or other incidents.
d) Protecting their passwords and other devices (e.g. keys, access cards, access tokens) that enable access to RGP information assets.

6 Information Security Management Program

The RGP's Information Security Management Program will include the following components:

1. Provision of privacy and security awareness training to all employees, volunteers, and contractors of the RGP.

2. Monitoring and audit of access to the RGP Registry System and compliance with the Information Security Policy.

3. Investigation and response to security and privacy incidents, including unauthorized access attempts or attempts to compromise the RGP Registry System.

4. Provision of ongoing guidance to RGP staff, volunteers, and contractors on matters related to information security.

5. Definition of security requirements for services provided by organizations (e.g. technology vendors) that support the RGP Registry System, and monitoring to ensure compliance with those requirements, policies and directives.

6. Establishment of agreements with suppliers and vendors of products and services, ensuring that suppliers and vendors comply, as required, with the Information Security Policies and standard operating procedures (SOPs).

7. Development, testing and maintenance of a business continuity plan for the RGP Registry System to ensure continued delivery of health services in the event of a system failure.

8. Determination and classification of the sensitivity of PHI and critical RGP Registry System assets to ensure that adequate security safeguards commensurate with the sensitivity of the PHI and critical system assets are implemented.

7 Access to the RGP Registry System

1. The RGP Registry System will apply role-based access control.

2. Role definitions for users of the RGP Registry System will be defined by the RGP. End-users and operators will be assigned roles by their managers.

3. Access to the RGP Registry System will be granted on a need-to-know basis, based on the end-user's role.

4. All end-user activity, including access to the RGP Registry System, is subject to monitoring and audit by the RGP.

8 Acceptable Use of RGP Systems and Information Assets

1. RGP system resources and information will only be used for purposes authorized by the RGP.

2. PHI will only be used and disclosed for those purposes defined in the Information Privacy Policy. These purposes include:

   a) The provision of healthcare, or assisting with the provision of healthcare, to individuals.
   b) Planning, evaluating, monitoring and delivering programs of the RGP and participating organizations.
   c) Health research subject to the requirements of PHIPA and its regulation.
   d) The provision of summary and statistical reports that do not include PHI, to support the management of the Ontario health care system (including the provision of summary and statistical reports to the RGP's funders).

3. Agents of the RGP shall not access, post, transmit or otherwise distribute material which is unlawful, harassing, libelous, defamatory, profane, abusive, threatening, harmful, vulgar, obscene, sexually suggestive, hateful, invasive of another's privacy or otherwise objectionable. Employees, volunteers, or contractors of the RGP shall not access inappropriate Internet sites including those that contain sexually explicit or pornographic material, gambling activities, or materials which could be considered harassing, degrading or discriminatory by others.

9 Encryption

1. The RGP shall ensure that PHI stored on portable devices such as laptop computers, tablets, personal digital assistants, or smartphones is encrypted using strong encryption.

2. The RGP shall ensure that PHI communicated across public or insecure networks is encrypted using strong encryption.

10 Violations of this Information Security Policy

1. Any violation of this Information Security Policy by an employee of the RGP is subject to disciplinary sanctions as determined by the RGP up to and including dismissal.

2. Any violation of this Information Security Policy by a supplier, vendor or contactor or their respective employees and agents, is subject to remedies identified in the agreement or contract. The RGP may request the removal of a supplier, vendor or contractor employee who has violated this Information Security Policy.

3. Any violation of this Information Security Policy by an employee or agent of a Participating Organization is subject to the disciplinary policies and procedures of the Participating Organization. The RGP may suspend individual users of the RGP Registry System until any issues are resolved by the Participating Organization.

11 Contact

For more information about this Information Security Policy, please contact:

Director of Operations
Regional Geriatric Program of Toronto
2075 Bayview Ave., Room H478
Toronto, On, M4N 3M5
http://rgp.toronto.on.ca/
Phone: (416) 480-6100 ext. 3341
Fax: (416) 480-6068

RGP REGIONAL GERIATRIC PROGRAM OF TORONTO

2075 Bayview Avenue, H478, Toronto, ON M4N 3M5 | 416-480-6026 | F: 416-480-6068 | www.rgp.toronto.on.ca