Information Privacy and Security Incident Management Policy

Reviewed Date		**Number**	*IM0108*
Revised Date	September 24, 2020	**Approved Date**	September 20, 2006

Introduction

Health Unit agents collect, use and disclose personal information including personal health information in the management and delivery of public health services. A privacy or security incident is an event occurring within a health unit program or system that

- places the privacy of personal information or personal health information at risk and/or
- places the confidentiality, integrity or availability of personal and personal health information at risk

and is attributable to the actions of one or more individuals, an agency process or malicious software.

A privacy breach is an incident that involves **the unauthorized** collection, use (access, storage and transmission), modification, disclosure or destruction of personal or personal health information whether in physical (paper) or electronic form. A privacy breach can also be a consequence of faulty business procedure or operational break-down e.g. information lost, misplaced or inappropriately retained. See Appendix A for examples of incidents and breaches.

The Simcoe Muskoka District Health Unit takes the privacy and security of information in its custody and under its control seriously and takes all reasonable steps to ensure that personal and personal health information in its custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal. Safeguards include requiring administrative, technical and physical controls to ensure the security and confidentiality of personal and personal health information.

Purpose

The purpose of this policy is to inform the Health Unit's Board of Health members, employees, students, volunteers, consultants (collectively defined as Health Unit *agents*) and members of the public of the rights and obligations of the Health Unit and the public in relation to breach and incidents related to personal health, and personal health information. This policy does not apply to labour relations or employment information associated to SMDHU

Legislative Authority

- the *Personal Health Information Protection Act, 2004* (PHIPA) and its regulations;

- the *Health Protection and Promotion Act*, 1990 and its regulations;
- the *Regulated Health Professions Act, 1991* (RHPA) and its regulations;

Policy Definitions and Interpretation

For the purposes of this Policy:

"agent" means a person that, with the authorization of the Medical Officer of Health as a Health Information Custodian (HIC), acts for or on behalf of the HIC in respect of personal health information for the purposes of the HIC, and not for the agent's own purposes, whether or not the agent has the authority to bind the HIC, whether or not the agent is employed by the HIC, and whether or not the agent is being remunerated;

"health information custodian (HIC)" means a person or organization listed in PHIPA that has custody or control of personal health information as a result of or in connection with performing the person's or organization's powers or duties or work, and includes a medical officer of health of a board of health within the meaning of the *Health Protection and Promotion Act , 1990.*

"PHIPA" – means *Personal Health Information Protection Act, 2004*

"personal health information" means identifiable information about an individual in oral or recorded form, if the information:

- relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family,
- relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual,
- is a plan of service within the meaning of the Long-Term Care Act, 1994 for the individual,
- relates to payments or eligibility for health care in respect of the individual,
- relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance,
- is the individual's health number, or
- identifies an individual's substitute decision-maker.

Personal health information includes identifiable information that is not personal health information but that is contained in a record that contains personal health information, and is not severed (mixed records).

Policy

The Medical Officer of Health will ensure that the Health Unit takes all reasonable steps to safeguard personal and personal health information resources in its custody and control, and to respond in a timely manner to security and privacy incidents.

Procedures

Supervisors will ensure that their staff are oriented to, and aware of, their obligations under this policy. The Privacy Officer will ensure that all Health Unit staff receive privacy and security awareness training, including guidance on responding to potential or actual privacy or security incidents or breaches. As a minimum steps will include:

- intake and documentation of incident reports
- containment and resolution of incidents and breaches
- notification to affected clients
- notification to other affected stakeholders as required by policy or contract
- incident investigation and continuous quality improvement
- reporting breaches to the Ontario Information and Privacy Commissioner as required by law.

If records of information systems containing personal and/or personal health information are lost, stolen, disclosed to, or accessed by an unauthorized person, the Privacy Officer will ensure that the individual(s) affected are notified of the breach at the first reasonable opportunity,

The Privacy Officer will ensure that other parties potentially impacted are informed of the security incident and/or privacy breach as required by legislation, contract or agency policy.

Health Unit employees will take all necessary measures to safeguard information resources and to prevent unauthorized collection, use, disclosure or disposal of personal and personal health information. Health Unit employees will document and report all information privacy and security incidents to their immediate supervisor.

Supervisors, working with the Privacy Officer, the Manager of IT and Infrastructure, and others as required will take immediate action to respond to and resolve all identified information privacy and security incidents and breaches according to documented incident and breach management procedures. Third parties service providers will be obligated through their agreements with the Health Unit to assume incident management responsibilities where required to support the Health Unit in addressing information privacy and security incidents.

The Privacy Officer will conduct an investigation of each documented privacy or security incident that occurs in the Health Unit and will monitor the implementation of any recommendations in the incident investigation.

An annual report of Privacy and Security Incidents along with actions taken and lessons learned will be prepared by the Privacy Officer and presented to Executive Committee and the Board of Health.

Procedures

Privacy and Information Management Procedures Manual

Related Policies

IM0101 Personal Health Information and Privacy Policy
IM0101 SMDHU Privacy Statement
IM0121 Transporting Records Policy

Related Forms

IM0108 (F1) Report of Information Privacy or Security Incident

Final Approval Signature: _____

Review/Revision History:

September 2020 – Policy Revision

September 2010 Policy re-numbered, previous number A1.048

Appendix A

A **Privacy Incident or Breach** could include:

- a circumstance where personal information or personal health information is subject to unauthorized access, use, or disclosure or unauthorized copying, modification or disposal
- a contravention, through the actions of a health unit employee or contractor, of the privacy rights of an individual
- a contravention of health unit privacy policies and procedures
- a contravention of privacy-related terms and conditions in agreements with third party service providers

A **Security Incident** could include:

- a contravention of health unit security policies and procedures
- a contravention of the security-related terms and conditions in agreements with third party service providers
- an attack of malicious code
- unauthorized access to information or physical systems
- inappropriate usage of information or physical assets
- unauthorized changes to systems
- system, software or hardware malfunctions