## *Information Privacy and Security Assessment*

| | | | |
|---|---|---|---|
| **Reviewed Date** | | **Number** | *IM0119* |
| **Revised Date** | | **Approved Date** | *September 23, 2009* |

### *Introduction*

The Board of Health and Medical Officer of Health are collectively responsible for ensuring policies and practices are in place to protect the privacy and security of personal information and personal health information collected by the Simcoe Muskoka District Health Unit. Privacy Impact Assessments (PIA) and Threat Risk Assessments (TRA) are tools used to engage stakeholders in the privacy and security assessment of new or changing information systems and technologies in order to make informed decisions regarding the most appropriate and cost effective safeguards for the information and agency systems.

### *Purpose*

The purpose of this policy is to inform Simcoe Muskoka District Health Unit Board of Health members, employees, students, volunteers and contractors of the standard process for assessing new and changing information systems and technologies for potential threats or risks to information privacy and technology assets.

### *Legislative Authority*

Personal Health Information Protection Act, 2004 (PHIPA)
Municipal Freedom of Information and Protection of Privacy Act, 1990 (MFIPPA)

### *Policy Definitions and Interpretation*

***Personal Health Information*** means identifying 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 Information*** means recorded information about an identifiable individual, including:

- information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
- information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
- any identifying number, symbol or other particular assigned to the individual,
- the address, telephone number, fingerprints or blood type of the individual,
- the personal opinions or views of the individual except if they relate to another individual,
- correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,
- the views or opinions of another individual about the individual, and
- the individual's name if it appears with other personal information including personal health information relating to the individual or where the disclosure of the name would reveal other personal information including personal health information about the individual.

***Privacy*** the right of individuals to control their information.

***Process Owner*** is the non-IT agency staff lead for a solution with responsibility of directing IT as to support and Disaster Recovery Plans (DRP) requirements

***Security*** encompasses the concepts of Confidentiality, Integrity and Access with respect to personal information. It requires custodians of personal information to take steps that are reasonable in the circumstances to protect information within its custody and control against theft, loss, unauthorized copying, modification, use, disclosure or disposal.

## *Policy*

A Privacy Impact Assessment and Threat Risk Assessment will be conducted on all new information systems and technologies and existing information systems and technologies that are used in the collection, use, management and disclosure and/or destruction of personal information including personal health information.

The Privacy Officer, Service Director and IT Supervisor will review the findings and recommendations of the assessments indicate by their signature acceptance of the threats and risks posed as well as the adequacy of safeguards to be put into place.

The Service Director, Privacy Officer and IT Supervisor must sign off on the PIA/TRA **prior** to the implementation of a new system or the implementation of significant change to an existing system.

The Administrative Coordinator Corporate Service maintains the PIA/TRA records and brings forward for review and final confirmation of items for action identified prior to implementation.

## *Procedures*

1. The Process Owner will initiate the assessment with a request to the Privacy Office for forms and guidance. An assessment may also be initiated by the Privacy Officer through the Service Director to the Process Owner.
2. Upon request from the Process Owner, the IT Supervisor will assign a technology team member to act as the PIA Technical Lead to assist the Process Owner with the complete and document the assessment using the form IM0119 (F1) Privacy Information Assessment/ Threat Risk Assessment
3. The PIA Technical Lead will review the completed assessment with the IT Supervisor for input and endorsement of the assessment and proposed safeguards.
4. The Process Owner will organize a meeting to conduct the formal review of the assessment findings and recommendations by the Service Director, Privacy Officer and IT Supervisor.
5. The Service Director, IT Supervisor and Privacy Officer will respond in one of three ways:
    a. Unconditional Approval - acceptance of the identified risks to information privacy and security and the cost effectiveness of proposed safeguards.
    b. Conditional Approval - acceptance of the identified risks to information privacy and security with the proviso that additional safeguards be put in place within a defined period of time.
    c. Project Refusal – signifies one of the three is unable to accept the risks to information privacy and security posed by the system or technology because they pose a significant risk to the organization.
6. The results of the review are documented:
    a. For Unconditional Approval, the PIA/TRA is signed by Service Director, Privacy Officer and IT Supervisor.
    b. For Conditional Approval, the Service Director, Privacy Officer and IT Supervisor sign the PIA/TRA identifying the additional safeguards to be put in place and the timelines within which this will occur.
    c. In the event of a Project Refusal the system or technology cannot be implemented or plans for retiring the system or technology will be identified.
7. The Process Owner provides the final documentation to the Administrative Coordinator – Corporate Service for filing. The Administrative Coordinator – Corporate Service will flag Projects receiving Conditional Approval for follow up within the defined period of time.
8. Decisions arising from this process can be appealed to the Medical Officer of Health.
9. The Administrative Coordinator Corporate Services brings forward assessments with conditional approval to the Privacy Officer for review and follow up on items outstanding. Approval of a system can be withdrawn by the Privacy Officer, Service Director or IT Supervisor should conditions not be met within the time period specified.

## *Forms*

IM0119 (F1) Privacy Information Assessment/ Threat Risk Assessment

## *Related Policies*

Policy IM0101 Personal Information Including Personal Health Information Privacy – Principles
Policy IM0102 Personal Information Including Personal Health Information Privacy – Accountability
Policy IM0103 Personal Information Including Personal Health Information Privacy – Consent
Policy IM0104 Personal Information Including Personal Health Information Privacy – Collection & Use
Policy IM0105 Personal Information Including Personal Health Information Privacy – Disclosure
Policy IM0106 Personal Information Including Personal Health Information Privacy – Access
Policy IM0107 Personal Information Including Personal Health Information Privacy – Correction
Policy IM0108 Personal Information Including Personal Health Information Privacy – Privacy Breach

***Final Approval Signature:*** _____

Review/Revision History:
September 2010 Policy re-numbered, previous number A1.051