Personal Information Including Personal Health Information Privacy – Privacy Breach

Reviewed Date		**Number**	*IM0108*
Revised Date	*February 9, 2000*	**Approved Date**	*August 23, 2000*

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 breach happens when personal information is collected, used, disclosed or disposed of in a manner that does not comply with applicable privacy legislation and the policies of the agency.

The most common privacy breaches are:

- unauthorized collection of personal health information (information is collected without consent or legal authority),
- unauthorized disclosure of personal health information through:
    - loss (a file is misplaced),
    - theft (a laptop is stolen), or
    - mistake (a letter addressed to one person gets faxed to the wrong person), and
    - unauthorized or unsecured disposal of personal health information (an unshredded file is left in the garbage).

Purpose

The most common privacy breaches are:

- unauthorized collection of personal health information (information is collected without consent or legal authority),
- unauthorized disclosure of personal health information through:
    - loss (a file is misplaced),
    - theft (a laptop is stolen), or
    - mistake (a letter addressed to one person gets faxed to the wrong person), and
- unauthorized or unsecured disposal of personal health information (an unshredded file is left in the garbage).

Legislative Authority

Policy Definitions and Interpretation

Policy

It is the responsibility of Health Unit agents in possession of a record of personal information including personal health information to ensure the security of that record and to take the necessary measures to prevent unauthorized collection, use, disclosure or disposal of the record.

Health Unit agents will document and report all privacy breaches to their immediate supervisor. Supervisors will take immediate action to identify the scope of the breach and to contain the breach.

If a record containing personal information including personal health information has been lost, stolen or accessed by unauthorized personnel the individual(s) will be informed of the privacy breach.

The Associate Director of Corporate Service (ADCS) is responsible for ensuring that individuals who were subject to a privacy breach are informed of the breach, for reviewing reports of all privacy breaches and recommending preventive action and for reporting to the Privacy Commission as required.

Procedures

A. Identifying and Containing a Privacy Breach:

1. If a record has been stolen the Health Unit agent will report the theft and the circumstances involved to the local police authority and then proceed to step 3.
2. If a record is missing (i.e. cannot be located when needed) or has been accessed by unauthorized personnel, the agent discovering the loss or unauthorized access (e.g. letter containing personal health information faxed to the wrong number).
3. The agent will notify his/her program manager immediately.
4. The manager/supervisor will review, with the agent the circumstances associated with the loss/theft, unauthorized access of the record. If it is determined that a record has come into the possession of a third party (e.g. through theft), the Medical Officer of Health will be notified of the circumstances both verbally and in writing.
5. The manager/supervisor, with the agent, identifies the extent of the privacy breach and take steps to contain it including:
    - retrieve the hard copies of any personal information including personal health information that has been disclosed.
    - ensure that the person who was not authorized to receive the information did not make or keep copies of the information and get that person's contact information in case you need to follow up.
    - determine whether the privacy breach allows unauthorized access to any other information (for example, through an electronic information system). Take all appropriate steps (for example, change passwords) to stop any further breaches.

6. The manager/supervisor with the agent and others as required (MOH, Director, Associate Director of Corporate Service) will determine what actions could be undertaken to avoid a re-occurrence.

B. Notification of a Privacy Breach

1. The program manager, with the agent member, and others as required (MOH, Director, Associate Director of Corporate Service) will:
    - Identify the people whose privacy has been breached.
    - Notify (by telephone or in writing) anyone whose privacy was breached (except for any of those who do not have the right to see or obtain their own information).
    - Specify what and how much information was affected.
    - Explain immediate and long-term steps taken to rectify the breach.
    - Note the unauthorized uses and disclosures in or linked to the affected records.

C. Reporting a Privacy Breach or Privacy Complaint

Reports of a privacy breach may be generated internally by Health Unit agents or may come as a complaint from the public.

1. The agent will complete a "Report of Privacy Breach" Form IM0108 (F1) report detailing:
    - essential identifying information of the person(s) whose privacy has been breached
    - the last known location of the record(s),
    - efforts made to locate the record(s),
    - circumstances related to the loss or discovery of unauthorized access
    - date last signed out and by whom and
    - other relevant information e.g. police report
    - outcomes and actions taken to notify the affected parties and address the reason for the breach.
2. The original of the report will be forwarded to the Service Director, who reviews the report and forwards to the Associate Director Corporate Service for filing in the Central Corporate file. A copy of the report will be retained by the agent and by the manager/supervisor. (If the record is subsequently located, a follow-up communication will be sent to the same people, and the new record will be merged with the recovered record).
3. The agent will create a new record and document the fact that the original record has been lost, as well as any information from the original record that can be accurately recalled. The "Breach of Security" report will be cross-referenced on the record.

D. Audit and Reporting on Breaches of Personal Privacy

1. On an annual basis, the ADCS will review and compile a report of the privacy breaches under the *Personal Health Information Protection Act, 2004* and the *Municipal Freedom of Information and Protection of Privacy Act, 1991*.
2. The ADCS will submit to executive committee the report along with a summary of actions taken to prevent future privacy breaches and recommendations for additional action.

3. The report will be reviewed by executive committee and response to recommendations documented.

The ADCS will provide the required information regarding privacy breaches to the Privacy Commission as part of a report submitted annually or upon request.

Related Forms

IM0108 (F1) Report of Privacy Breach

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 A1.048