CATEGORY:	**ORGANIZATIONAL: INFORMATION MANAGEMENT**
SUB-CATEGORY:	**PRIVACY**
GROUP:	
DISTRIBUTION:	**ALL STAFF/PHYSICIANS**
TITLE:	**PRIVACY BREACH PROTOCOL**

PURPOSE

To provide guidelines for employees/physicians in the event of a privacy breach.

POLICY

Western Health must respond to all privacy breaches. All employees/physicians must **immediately** notify the immediate manager and Regional Manager, Information Access and Privacy of all privacy breaches such that appropriate action may be taken to contain and respond to the situation. The Regional Manager, Information Access and Privacy will consult with the Regional Risk Manager/Patient Safety Advisor and other members of Western Health's management team as appropriate.

The manager/director in the department/unit/program/service where the breach occurred must ensure that an *Occurrence Report* form is completed and forwarded to the Risk Manager/Patient Safety Advisor as per policy 6-02-15 *Occurrence Reporting*.

As well, policy 6-02-16 *Disclosure of Occurrences* and the following documents prepared by the provincial Access to Information and Protection of Privacy (ATIPP) Office must be consulted when responding to a privacy breach. The Regional Manager, Information Access and Privacy must lead this process with the director/manager in the department/unit/program/service where the breach occurred. Please consult the document *Key Steps When Responding to a Privacy Breach* found in the guidelines section of this policy when investigating privacy breaches.

Policy 6-04-60 *Client Feedback: Compliments and Complaints* must also be consulted as necessary.

DEFINITIONS

Direct notification– This refers to notifying individuals who have been affected by a privacy breach through direct means including telephone, letter or in person.

Indirect notification – This refers to notifying individuals who have been affected by a privacy breach through indirect means including website information, posted notices, or the media.

Privacy breach - occurs when there is unauthorized and/or inappropriate access, collection, use, disclosure or disposal of personal information. Such activity is "unauthorized" if it occurs in contravention of the *Access to Information and Protection* of Privacy *Act (ATIPPA)*. The most common privacy breaches occur when personal information of customer, patients, clients or employees is stolen, lost or mistakenly disclosed. For example, a privacy breach occurs when a computer containing personal information is stolen or personal information is mistakenly emailed to the wrong person.

KEY WORDS

Privacy Breach
Privacy Breaches
Breach
Breaches
Privacy

GUIDELINES

APPENDIX A

KEY STEPS WHEN RESPONDING TO A PRIVACY BREACH

The following guidelines will be used in consultation with the Regional Manager, Information Access and Privacy when responding to privacy breaches:

Step 1: Contain the Breach

Immediate actions must be taken to contain the breach. Both these steps must take place in quick succession:

- **Contain the breach –** Immediately stop the unauthorized practice, recover the records, and correct weaknesses in physical security. If the breach is an unauthorized access to an IT asset, such as a computer, service or network, employees must shut down the affected asset and contact Information Systems immediately.

- **Immediately contact** the immediate manager/director and the Regional Manager, Information Access and Privacy.

Step 2: Evaluate the Risks

To determine what other steps are immediately necessary, assess the risks associated with the breach. Consider the following factors when assessing the risks:

Personal Information Involved

- What types of information are involved in the breach? Generally, the more sensitive the information, the higher the risk.

- Can the information be used for fraudulent of otherwise harmful purposes? (eg. Social Insurance Numbers and financial information may be used for identity theft).

Cause and Extent of the Breach

- What is the cause of the breach?
- Is there a risk of ongoing or further exposure of the information?
- How much information was collected, used or disclosed without authorization?
- What is the number of likely recipients?
- Is the information protected by encryption or other means?
- What steps have already been taken to minimize the harm?

Individuals Affected by the Breach

- How many individuals are directly affected by the breach?
- Who was affected by the breach: employees, citizens, clients?

Foreseeable Harm from the Breach

- Is there any relationship between the unauthorized recipients and the information involved in the breach?

What is the risk of harm to **affected individuals** as a result of the breach?

  - Security risk (e.g. physical safety)
  - Identity theft or fraud
  - Loss of business or employment
  - Hurt, humiliation, damage to reputation or relationships

- What is the risk of harm to the **public body** as a result of the breach?

  - Loss of trust in the public body or organization
  - Loss of assets
  - Financial exposure

- What is the risk of harm to the **general public** as a result of the breach?

  - Risk to public health
  - Risk to public safety

Step 3: Notification

Please refer to the *Privacy Breach Notification Assessment Tool* (Appendix B) for complete information on notification.

A key consideration in deciding whether notification is necessary is the mitigation of harm to any individuals whose personal information has been inappropriately collected, used or disclosed as a result of the breach.

The *Privacy Breach Notification Assessment Tool* (Appendix B) must be used to assess whether notification of affected individuals is required.

Notifying Affected Individuals

As mentioned above, notification of affected individuals must occur if it is necessary to avoid or mitigate harm to them. Some considerations in determining whether to notify individuals affected by the breach include:

- Contractual obligations requiring notification,

- Risks of identity theft or fraud (usually due to the type of information lost, such as Social Insurance Number or financial information),

- Physical harm (the loss puts an individual at risk of being stalked or harassed),

- Risk of hurt, humiliation or damage to reputation (eg. disciplinary or medical records being breached).

When and How to Notify of a Privacy Breach

When: If notification is to take place, it should occur as soon as possible following the breach. However, if the Regional Manager, Information Access and Privacy and the manager/director in the affected department/unit/program/service have contacted law enforcement authorities, it must determined from those authorities whether notification needs to be delayed in order not to impede a criminal investigation.

How: The preferred method of notification is direct (i.e. by phone, letter or in person) to affected individuals. Indirect notification (i.e. website information, posted notices, media) should generally only occur where direct notification could cause further harm, is prohibitive in cost and/or contact information is lacking. Using multiple methods of notification in certain cases may be the most effective approach.

What should be included in the notification?

Notifications must include the following pieces of information:

- Date of the breach,
- Description of the breach,
- Description of the information inappropriately accessed, collected, used or disclosed,
- The steps taken to date to mitigate the harm,
- Next steps planned, as well as any long term plans to prevent future breaches,
- Advice to the individual to mitigate further harm,
- Contact information of an individual within the public body who can answer questions or provide further information,
- The right of the individual to complain to the Office of the Information and Privacy Commission (OIPC), noting contact details.

Others to Contact

In consultation with the Regional Risk Manager/Patient Safety Advisor and other appropriate management as necessary, the manager/director in the department/unit/program/service where the breach occurred and the Regional Manager, Information Access and Privacy decide whether the following authorities or organizations also need to be informed of the breach:

- **Police:** If theft or other crimes are suspected.

- **Senior Privacy Analyst, ATIPP Office:** To provide advice or guidance in regard to the privacy breach.

- **Insurers or others:** If required by contractual obligations.

- **Professional or other regulatory bodies:** If professional or regulatory standards require notification.

- **IT Department:** If the breach is an unauthorized access to an IT asset, such as a computer, service or network, employees must shut down the affected asset and contact Information Systems immediately.

Step 4: Prevention

Once the immediate steps are taken to mitigate the risks associated with the breach, Managers/directors in the department/unit/program/service where the breach occurred, the Regional Manager, Information Access and Privacy and the Regional Risk Manager/Patient Safety Advisor will:

- Thoroughly investigate the cause of the breach. This could require a security audit of both physical and technical security,
- Develop or improve, as necessary, adequate long term safeguards against further breaches,
- Review policies and update them to reflect the lessons learned from the investigation,
- Audit at the end of the process to ensure that the prevention plan has been fully implemented, and
- Educate all employees/physicians to know the organization's privacy obligations under applicable laws (e.g. *ATIPPA*)

Approved By: Chief Executive Officer	Maintained By: Regional Manager, Information Access & Privacy
Effective Date: 18/March/2009	☐ Reviewed: ☑ Revised: 12/April/2010
Review Date: 12/April/2013	☐ Replaces: *(Indicates name and number of policy being replaced)* OR ☑ New