Centre for
Heart Lung Innovation
UBC and St. Paul's Hospital

# STANDARD OPERATING PROCEDURE

| | | | |
|---|---|---|---|
| **Title:** | **8.7 Managing Privacy Breaches** | | |
| **Procedure:** | **PR-0807(1)** | **Supercedes:** | **none** |
| **Originator and Date:** | **Jacqui Brinkman March 3, 2009** | **Effective Date:** | **03Mar2009** |
| **Review Frequency:** | **annually** | **Approved By:** | **The JHRC Privacy Team** |
| **Total Number of Pages: 5** | | | |

| **Revision History** | | |
|---|---|---|
| **Date** | **Reviewer** | **Summary of revision** |
| 19Apr2012 | Raquel Park/Joe Comeau | Update "iCAPTURE Centre" to "JHRC" |
| Aug 2013 | Raquel Park/Joe Comeau | Update "JHRC" to "HLI" |
| | | |
| | | |

## 1. BACKGROUND

As a public body and a steward of Personal Information, the Centre for Heart Lung Innovation is accountable for protecting the privacy and security of all Personal Information under its custody and control in accordance with existing legislation, public expectations and internationally accepted fair information practices. ***FOIPPA*** provides a framework for circumstances in which Personal Information may be collected, used or disclosed by all provincial public bodies. Other applicable best practice standards to which the HLI adheres include the ***TCPS*** and the ***CIHR Best Practices for Protecting Privacy in Health Research***.

## 2. PURPOSE

As a steward of personally identifiable data collected to support its research programs, the HLI must protect all Personal Information of research subjects/partners, patients/residents/clients and ensure that it is collected, used or accessed, retained and disclosed by the HLI only on a need to know basis and only for its intended purpose, as governed by ***FOIPPA***. The purpose of this policy is to ensure an effective and standardized management of privacy incidents where

Personal Information or other confidential or sensitive information has been lost, stolen or intentionally or inadvertently disclosed.

Effective internal controls and procedures will:

- minimize the potential risk to the HLI and its research subjects/partners, patients/residents/clients and staff;
- enable a prompt, effective and orderly response to privacy incidents;
- comply with the requirements of the FOIPPA; and
- prevent recurrence.

As indicated by the Privacy Commissioner of BC "costs should not be a determining factor when assessing the adequacy of security".

## 3. SCOPE

This policy applies to all staff or trainees working for, or associated with, the HLI and any of its affiliated Programs and Agencies that are covered by ***FOIPPA***. This policy also applies to any incident where research subject personally identifiable information or other confidential or sensitive information in the custody and/or control of the HLI is lost, stolen or intentionally or inadvertently disclosed contrary to the BC Freedom of Information and Protection of Privacy Act (FOIPPA). Protecting personal privacy is a fundamental matter that is integrated into HLI's organizational culture and into every research process.

## 4. POLICY STATEMENT

Personal Information will be collected, used, disclosed, retained and destroyed in accordance with ***FOIPPA*** and other relevant legislation. The CSA ***Model Code for the Protection of Personal Information*** principles form a foundation of best practice.

Any unauthorized access to, or collection, use, disclosure or disposal of Personal Information in the custody of the HLI is considered a "Privacy Breach". Such activity is considered to be "unauthorized" if it occurs in contravention of the BC Freedom of Information and Protection of Privacy Act (FOIPPA). The most common privacy breach happens when Personal Information of research subjects/partners, patients/residents/clients is lost, stolen or inadvertently disclosed. Intentionally viewing confidential information that is not necessary to perform an individual's role is considered a breach of confidentiality even if that information is not disclosed to another party. Confidential information must not be discussed in any physical location where others may overhear. Unapproved access or communication of confidential information constitutes a breach of privacy and confidentiality.

The HLI Privacy Team will promptly and thoroughly investigate and document all privacy incidents related to actual or potential breaches of confidentiality and will take timely and appropriate action to contain and diminish risk arising from a privacy breach. Privacy breaches

will be managed in accordance with the guidelines set out by the Office of the Information and Privacy Commissioner for British Columbia (OIPC), Ministry of Health and other generally accepted best practices.

All HLI members are expected to cooperate with Privacy Facilitator and Team and assist in a thorough and timely investigation of all privacy incidents. Failure by HLI staff, trainees or other members to comply with this Policy may result in disciplinary action including, but not limited to, the loss of computing privileges, loss of privileges as a student placement or termination of employment.

## 5. PROCEDURE

A key aspect of any privacy breach is immediate response and action to the breach. By adhering to the following steps, the HLI will not only minimize the risks associated with a privacy breach but will develop strategies to reduce future privacy breaches.

**1. Contain the Breach**

As soon as a privacy breach is identified it must be immediately contained and limited. Actions for HLI staff, trainees or other members to take include:

- contain the breach (i.e. stop the unauthorized practice, recover the records, change computer access codes, or improve physical security);
- notify Security (if applicable), the manager/leader of the affected department and the iCAPTURE Centre Privacy Facilitator;
- notify police and obtain a case number if theft or criminal activity is involved;
- if needed, assemble a team which includes the Privacy Facilitator to help respond to and manage the breach.

**2. Evaluate the Risks Associated with the Breach**

To determine a course of action for managing a privacy breach, assessment of the extent of risk to the Centre for Heart Lung Innovation, to the University of British Columbia (UBC), to Providence Health Care, to research subjects/partners and patients/residents/clients associated with the breach is necessary. Details to consider include:

- Type and sensitivity of personally identifiable information compromised (i.e. health information, contact information);
- The cause and extent of the unauthorized collection, use or disclosure including any potential further exposure of the information;
- Number of individuals affected and their relationship to HLI, UBC and PHC;
- Was the information lost or stolen and has the information been fully recovered;
- Accessibility to information (i.e. was information encrypted or password protected);
- Who was the recipient of the information and what is their relationship to the persons whose information has been compromised;

- Potential harmful uses of the Personal Information (i.e. fraud, risk to public health, loss of business or employment opportunities, embarrassment, damage to reputation or relationship); and
- Potential harm to the HLI, UBC or PHC (i.e. loss of public trust).

**3. Notification**

**Reporting the Privacy Breach:**

Staff, trainees or other HLI Centre members must immediately report any actual or potential theft, loss or disclosure of Personal Information or other confidential or sensitive information regardless of its format (i.e. verbal, written, electronic). All potential or actual privacy breaches must be reported to the Privacy Facilitator in accordance with this policy to ensure that appropriate steps are taken to manage the breach, to redress any harm that arises from the breach, and to prevent recurrence. Staff, students or other Centre members may report real or suspected breaches without any fear of reprisal.

Initial notification to the Privacy Facilitator or security team may be by telephone but must be followed as soon as possible by notification in writing. Details of the privacy breach to include in notification are:

- Date, time and location of the breach;
- Description of the breach (e.g. email, fax, theft, loss, etc.);
- Estimated number of persons affected;
- Name(s) and contact information of any person who was involved (including any witnesses);
- Name(s) of those notified of the breach and time of notification;
- Steps taken to contain the breach or potential breach.

Theft or loss of information storage devices (e.g. PC's, laptops, Blackberries, removable storage devices) or incidents where system access may be compromised must also be reported to the HLI Help Desk.

The Privacy Facilitator will report all privacy breaches to the HLI Operations Team and the HLI Executive and will:

- Ensure the breach has been contained;
- Investigate and document the extent and cause(s) of the privacy breach;
- Contact other departments/individuals within the HLI, UBC and PHC to assist in managing the breach or potential breach;
- Report the breach to the Leader, Information Access and Privacy of PHC.

**Notification to Affected Individuals:**

The HLI endorses the principle of disclosure when there has been a privacy breach. Notification to the individuals whose information was involved in the privacy breach or to other organizations

or groups affected by the breach may be required for legal, professional or contractual obligations and should occur as soon as possible following the breach.

The Privacy Team will evaluate the risks associated with the privacy breach or potential breach in consultation with the HLI Executive. If the privacy breach is assessed to be of significant risk or harm to the individuals about whom personal information was lost or disclosed, the Privacy Facilitator will:

- Promptly notify the OIPC and initiate processes to ensure appropriate disclosure to impacted individuals;
- Where there is a potential risk to individuals, notify the PHC Director, Risk Management and Patient Safety.
- Develop a communications plan;
- Make recommendations for and/or carry out notifications to affected individuals;
- Liaise with staff regarding OIPC reports and recommendations; and
- Prepare report and/or make recommendations to prevent recurrence.

**4. Prevention**

After immediate steps are taken to limit the privacy breach and associated risks, the Privacy Team will conduct a thorough investigation of the root cause of the breach. This may include a thorough security audit of all of our systems, both physical and technical, as well as a risk-based analysis of long-term safeguards to prevent further privacy breaches. All policies related to practices and procedures associated with the breach will be reviewed and updated based on the lessons learned and any OIPC recommendations. Staff, trainees and other HLI members will be provided with education and/or refresher training on privacy obligations related to the breach.

## 6. REFERENCES

A. Centre for Heart Lung Innovation Policies:
   - PR-0102: Defined Purposes: Centre for Heart Lung Innovation Data
   - PR-0701: Security Policy
   - PR-0901: Archiving, Retaining and Destroying Data
   - PR-1001: Centre for Heart Lung Innovation Privacy Policy

B. CSA ***Model Code*** Principle #8 Openness.

C. Providence Health Care Policy CPF1600: Managing Privacy Breaches. Approved Date: February 2008 from PHC Corporate Policy Manual.

D. OIPCBC Key Steps in Responding to Privacy Breaches (June 2006) http://www.oipcbc.org/pdfs/Policy/Key_Steps_Privacy_Breaches(June2008).pdf

E. OIPCBC Physicians & Security of Personal Information (June 2006)
http://www.oipc.bc.ca/pdfs/private/PhysicianSecurityofpersonalinformation.pdf

F. OIPC of BC Privacy Breach Reporting Form (November 2006)
http://www.ehip.ca/2006/presentations/2006/Tully_PrivacyBreachForm(Nov2006).pdf