

POLICY TITLE

**CONFIDENTIALITY AND SECURITY
OF PERSONAL INFORMATION**

AUTHORIZATION

Vice President, Corporate Services and
Chief Financial Officer

DATE APPROVED

October 2003

DATE REVISED

August 2005

Personal information is accessed on a need to know basis and is used only for its intended purpose as governed by British Columbia's *Freedom of Information and Protection of Privacy Act (FOIPPA)*.

Personal information as defined by FOIPPA can be any recorded information about an identifiable individual (excluding contact information). Examples of personal information include but are not limited to:

- The individual's name provided with home address and/or home telephone number;
- The individual's race, national or ethnic origin, colour or religious beliefs or associations;
- The individual's age, sex, sexual orientation, marital status or family status;
- An identifying number, symbol or other particular assigned to the individual;
- The individual's fingerprints, blood type or inheritable characteristics;
- Information about the individual's health care history including a physical or mental disability;
- Information about the individual's educational, financial, criminal or employment history;
- Anyone else's opinions about the individual; and,
- The individual's personal views or opinions except if they are about someone else.

Personal information can be recorded in any format including books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means.

POLICY

All personal information concerning patients / residents / clients and employees / physicians / volunteers is confidential and is only to be used by individuals who require access to it in order to provide direct service to the person to whom the information belongs or to follow up for quality of care review. Personal information required for any other reason requires consent of the individual or must meet conditions set out in Procedure Item 5.

All paper documents or electronic storage media containing personal information are the property of the Fraser Health Authority but the information belongs to the person about whom the information is recorded.

POLICY TITLE

**CONFIDENTIALITY AND SECURITY
OF PERSONAL INFORMATION**

AUTHORIZATION

Vice President, Corporate Services and
Chief Financial Officer

DATE APPROVED

October 2003

DATE REVISED

August 2005

Physical security of personal information (as defined in FOIPPA) is the responsibility of the individual or area holding the records. This includes information stored in electronic media as well as any information held in paper or other format(s). Original documents may not be removed from a site except in the case of a subpoena or in specific circumstances where the original record is required for continuity of care or the operational requirements of the Fraser Health Authority. Original records may not be removed from the site for chart completion.

Security of the network is the responsibility of the Information Management portfolio. Every person using the network must be authorized to access it and ensure confidentiality procedures and principles are followed. Usage of the Fraser Health Authority's information systems may be monitored to support operational, maintenance, auditing, security and investigative activities.

The Fraser Health Authority's communication (e-mail) system is not encrypted and offers little or no protection for personal information. If personal information must be transmitted outside of the Fraser Health Authority, approved protection technologies, must be employed to protect the information as outlined in the Fraser Health Authority's Electronic Communications Policy.

In order to protect the privacy of a third party whose personal information may appear on a record, paper or electronic, any physician or staff member wishing to access his or her own personal information must follow the appropriate process to request access to the information. See Procedure Item 10.

Fraser Health Authority employees (this term includes volunteers and service providers) have an obligation to report any unauthorized disclosures or demands for disclosure from outside of Canada, including subpoenas, warrants, or court orders, to the Fraser Health Authority's Information Privacy Office. Employees are protected under FOIPPA and can not be disciplined for reporting or refusing to process unauthorized disclosures or foreign demands for disclosure.

PROCEDURE

1. Confidential information is not to be copied, transferred, verbally transmitted, printed, transmitted, altered or used in any other way unless appropriate consent or authorization has been given in accordance with the Fraser Health Authority's policies and procedures, legislation, statutes and professional practice requirements.

POLICY TITLE

**CONFIDENTIALITY AND SECURITY
OF PERSONAL INFORMATION**

AUTHORIZATION

Vice President, Corporate Services and
Chief Financial Officer

DATE APPROVED

October 2003

DATE REVISED

August 2005

2. All new employees (this term includes volunteers and service providers), physicians, students and research staff are required to sign a *Confidentiality Acknowledgement* in regard to their professional responsibilities related to confidentiality of personal information. Students will sign the statement individually or as part of their affiliation agreement. No researcher will be given access to staff or patient/resident/client records until a *Confidentiality Acknowledgement* is signed.
3. Unapproved access or communication of confidential information constitutes a breach of confidentiality. Should an investigation determine that a breach of confidentiality has occurred, the employee, volunteer, student or physician will be subject to discipline, up to and including termination of employment or privileges.
4. Unauthorized disclosures or demands for disclosure from outside of Canada, including subpoenas, warrants, or court orders, must be reported to the Fraser Health Authority's Information Privacy Office.
5. Designated staff may release personal information if authorization has been given by the patient/resident/client, if its release meets applicable sections of the FOIPPA or is requested through subpoena, court order or other legislation.
6. Any individual using material for teaching, research, public education or other secondary purpose must meet the requirements for accessing and using the information set out in the FOIPPA.
7. Any third party (such as other health care agencies, affiliates, consultants, vendors or researchers) requiring access to personal information for service purposes agrees to maintain confidentiality as a condition of the contract being awarded. Maintenance of confidentiality and consequences of breach are included in all contracts.
8. A personal user ID and password for accessing any information is equivalent to a legal signature.
 - Fraser Health Authority employees (this term includes volunteers and service providers), physicians with privileges, students and all other individuals authorized to access information through Fraser Health Authority's computerized information systems are responsible for all activity performed with their personal user IDs. The transfer of a user's ID and password to another user does not alter the responsibility of the person who owns the ID and password. Disclosing the personal user ID or password exposes an individual to the responsibility of the actions the other individual may take with the personal user ID.
 - Similarly, unless expressly authorized by the owner of a personal user ID or password, employees are forbidden from performing any activity with another employee's ID.

POLICY TITLE

**CONFIDENTIALITY AND SECURITY
OF PERSONAL INFORMATION**

AUTHORIZATION

Vice President, Corporate Services and
Chief Financial Officer

DATE APPROVED

October 2003

DATE REVISED

August 2005

- Any individual who has reason to believe that his/her personal user ID has been compromised will contact their immediate supervisor, manager or designated Fraser Health Authority resource. If necessary, a new user code will be issued.
 - After completing work at a device (e.g. terminal, personal computer, or wireless device) connected to the Fraser Health Authority's computer network, all users must log out or use a password protected screen saver to prevent unauthorized access into the system.
9. Destruction of records is performed within provincial standards and/or guidelines.
 10. Fraser Health Authority employees (this term includes volunteers and service providers), physicians, students and all other individuals wishing to access their own health records must follow established procedures within Health Records for clinical files, Human Resources for personnel files and Medical Administration for medical staff information.
 11. Collection of information for research purposes must meet the standards as outlined by the Fraser Health Research Ethics Board and Section 35 of the Freedom of Information Protection of Privacy Act.

REFERENCES

- Corporate Privacy Impact Assessment Tool - Ministry of Management Services, Corporate Privacy and Information Access Branch
- Family and Child Service Act
- Fraser Health Authority Policy - Electronic Communications
- Freedom of Information and Protection of Privacy Act
- Guidelines to Promote the Confidentiality and Security of Automated Health Record Information, COACH, 1995
- Hospital Act
- Hospital Insurance Act
- Principles and Guidelines for Access to and Release of Information, Canadian Health Records Association, 1995
- Recorded Information Management Manual (RIMM) – Ministry of Management Services, Corporate Records Management Branch
- Storage and Disposal of Health Care Records in British Columbia - Dr. Shaun Peck