POLICY TITLE

CONFIDENTIALITY AND SECURITY OF PERSONAL INFORMATION

AUTHORIZATION	DATE APPROVED	DATE REVISED
Vice President, Information Management	October 2003	August 2005 January 2010 February 2011

1.0 INTRODUCTION AND SCOPE

This policy provides consistent standards and practices to ensure that Fraser Health employees are aware of and acknowledge the legal and ethical obligation and consequences of not adhering to such obligations to protect personal information. This policy applies to personal information and other confidential information under the custody and control of Fraser Health or under the custody and control of any other Health Organization or Collaboration Organization in British Columbia (or its affiliates) which Fraser Health employees have access to in the delivery of a common or integrated program.

2.0 POLICY

All personal information concerning Fraser Health 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, to perform duties legislated under the Public Health Act or to follow up for quality of care review. All Fraser Health paper documents or electronic storage media containing personal information are the property of Fraser Health but the information belongs to the person about whom the information is recorded.

Physical security of Fraser Health personal information and other confidential information 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 Fraser Health. Original records may not be removed from the site for chart completion.

Security of the Fraser Health network is the responsibility of the Information Management portfolio. Every person using the network must be authorized to access it and ensure privacy and security related policies and procedures are followed. The usage of Fraser Health information systems may be monitored to support operational, maintenance, auditing, security and investigative activities.

The Fraser Health communication (e-mail) system is not encrypted and offers little or no protection for personal information. If personal information or other confidential

POLICY TITLE

CONFIDENTIALITY AND SECURITY OF PERSONAL INFORMATION

AUTHORIZATION	DATE APPROVED	DATE REVISED
Vice President, Information Management	October 2003	August 2005 January 2010 February 2011

information must be transmitted outside Fraser Health, approved protection technologies must be employed to protect the information as outlined in the Fraser Health Electronic Communications Policy.

In order to protect the privacy of a third party whose personal information may appear on a record, paper or electronic media device, 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.

Fraser Health employees have an obligation to report any unauthorized disclosures or demands for disclosure of personal information from outside of Canada including subpoenas, warrants or court orders to the Fraser Health Information Privacy Office. Employees are protected under the Freedom of Information and Protection of Privacy Act (FIPPA) and can not be disciplined for reporting or refusing to process unauthorized disclosures or foreign demands for disclosure.

Procedures For Working With Personal And Other Confidential Information

1. Personal and other confidential information is not to be copied, transferred, verbally transmitted, printed, altered or used in any other way unless appropriate consent or authorization has been given in accordance with Fraser Health policies and procedures, legislation, statutes and professional practice requirements.
2. All Fraser Health employees, 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. Unapproved access or communication of personal and other 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.
3. All unauthorized disclosures of personal information or demands for disclosure of personal information from outside of Canada including subpoenas, warrants or court orders must be reported to the Fraser Health Information Privacy Office.

POLICY TITLE

CONFIDENTIALITY AND SECURITY OF PERSONAL INFORMATION

AUTHORIZATION	DATE APPROVED	DATE REVISED
Vice President, Information Management	October 2003	August 2005 January 2010 February 2011

4. Designated staff may release personal information if authorization has been given by the patient/resident/client/employee/physician/volunteer, if its release meets applicable sections of the FIPPA or is requested through subpoena, court order or other legislation.

5. Any individual using personal information for teaching, research, public education or other secondary purpose must meet the requirements for accessing and using the information set out in the FIPPA.

6. Researchers are authorized to have access to staff or patient/resident/client records through a formal process that includes approval from the Fraser Health Research Department and the Fraser Health Information Privacy Office.

7. Collection of personal information for research purposes must meet the privacy and security standards as outlined by the Research Ethics Board and/or Section 35 of the Freedom of Information Protection of Privacy Act.

8. Any third party, such as other health care agencies, affiliates, consultants, vendors or researchers, requiring access to personal information and other confidential information for service purposes and other purposes permitted under FIPPA, agrees to maintain confidentiality as a condition of the contract being awarded. Maintenance of confidentiality and consequences of breach are included in all contracts.

9. A personal user identification (ID) and password for accessing any information is equivalent to a legal signature.
   - Fraser Health employees (this term includes volunteers and service providers), physicians with privileges, students and all other individuals authorized to access information through Fraser Health's computerized information systems are responsible for all activity performed with their personal user ID. 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	DATE APPROVED	DATE REVISED
Vice President, Information Management	October 2003	August 2005 January 2010 February 2011

- Any individual who has reason to believe that his/her personal user ID has been compromised must contact the Service Desk. The Service Desk can be contacted by email: servicedesk@fraserhealth.ca or by phone at (604) 585-5544. If necessary, a new user code will be issued.
- After completing work at a device (i.e. terminal, personal computer or wireless device) connected to the Fraser Health computer network, all users must log out or lock the computer screen to prevent unauthorized access into the system.

10. Destruction of all records is performed within Provincial standards and/or guidelines.

11. Fraser Health 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.

3.0 DEFINITIONS

Contact Information is information that enables an individual at a place of business to be contacted and includes the name, position title, business telephone number, business address, business email or business fax number of the individual.

Collaboration Organization means any Health Organization with which Fraser Health is engaged in the delivery of a common or integrated program or service.

Health Organization means any Health Authority in British Columbia or its affiliates.

Other Confidential Information is the information provided to, collected or created by Fraser Health or a Collaboration Organization, which may or may not contain information on an identifiable individual, in the course of the business operations of the Fraser Health or such Collaboration Organization.

Personal Information is any recorded information about an identifiable individual (excluding contact information). Examples of personal information include but are not limited to:

POLICY TITLE

CONFIDENTIALITY AND SECURITY OF PERSONAL INFORMATION

AUTHORIZATION	DATE APPROVED	DATE REVISED
Vice President, Information Management	October 2003	August 2005 January 2010 February 2011

- 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.

4.0 REFERENCES

- Child, Family and Community Service Act
- Fraser Health - Confidentiality Acknowledgement Document
- Fraser Health Policy - Electronic Communications
- Fraser Health Policy – Research - Ethical Conduct of Research and Other Studies Involving Human Subjects
- Freedom of Information and Protection of Privacy Act (FIPPA)
- 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

POLICY TITLE

CONFIDENTIALITY AND SECURITY OF PERSONAL INFORMATION

AUTHORIZATION	DATE APPROVED	DATE REVISED
Vice President, Information Management	October 2003	August 2005 January 2010 February 2011

- Public Health Act
- Recorded Information Management Manual (RIMM) – Ministry of Management Services, Corpor1ate Records Management Branch
- Storage and Disposal of Health Care Records in British Columbia - Dr. Shaun Peck