		Page 1 of 6
POLICY TITLE **PRIVACY AND SECURITY REQUIREMENTS FOR MOBILE DEVICES**		**NUMBER** 02-774
AUTHORIZATION Vice President, Planning, Informatics and Analytics	**DATE APPROVED** November 28, 2017	**CURRENT VERSION DATE** October 19, 2017

DATE(S) REVISED / REVIEWED SUMMARY

Version	Date	Comments / Changes
1.0	January 2010	Initial policy released
2.0	October 2017	- Updated, expanded policy regarding Mobile Devices Not Owned by Fraser Health and enrolled with Fraser Health's mobile device management system - Rewording and consistency with newer policy wording - Additional statements moved from Secure Messaging as they pertain to all uses of mobile devices. - Storage devices removed as this is a separate policy. - Title of policy changed from Privacy and Security Requirements for Laptops, Notebooks, Blackberries and other Mobile Technology.

INTENT / PURPOSE

The Privacy and Security Requirements for Mobile Devices Policy protects Fraser Health Confidential Information from loss or unauthorized disclosure.

This policy is specific to mobile devices and is in addition to the general privacy and security policies of Fraser Health.

SCOPE

This policy applies to both Corporate Mobile Devices and Personal Mobile Devices used to access, process and/or store Fraser Health Confidential Information.

POLICY

General

Fraser Health Confidential Information stored on Mobile Devices is the property of Fraser Health.

- Mobile Devices may not be used to access, process or store Fraser Health Confidential Information unless enrolled with an approved Fraser Health Mobile Device program.
- Fraser Health staff and their personal devices must meet the eligibility requirements of the specific Fraser Health Mobile Device program.
- Fraser Health staff must agree to the *Terms of Use* as specified in the Mobile Device Program.
- Fraser Health reserves the right to de-enroll any Mobile Device at any time to the absolute discretion of Fraser Health.

All Fraser Health staff using a Corporate or Personal Mobile Device that accesses Fraser Health Systems or Data must review this policy prior to issue or enrollment. It is the responsibility of the business area to ensure that this policy is made available and read by each Fraser Health staff member prior to the Mobile Device being issued or enrolled.

		Page 2 of 6
POLICY TITLE **PRIVACY AND SECURITY REQUIREMENTS FOR MOBILE DEVICES**		**NUMBER** 02-774
AUTHORIZATION Vice President, Planning, Informatics and Analytics	**DATE APPROVED** November 28, 2017	**CURRENT VERSION DATE** October 19, 2017

Safeguarding Mobile Devices and Fraser Health Confidential Information
Fraser Health Confidential Information stored on any Mobile Device must be password protected, encrypted and stored only for the time period required to complete a task, in accordance with Fraser Health policies.

Fraser Health staff is responsible for taking reasonable care when accessing Fraser Health Confidential Information in public to guard against inadvertent disclosure. Mobile Devices must not be left unattended in unsecure locations.

Mobile Device users are responsible for complying with the following Fraser Health policies and their associated standards:

- Access Control – Policy
- Audit of Electronic Health Information Access – Policy
- Confidentiality and Security of Personal Information – Policy
- Electronic Communications – Policy
- Managing Privacy Breaches – Policy
- Terms of Use for applicable Fraser Health Mobile Device program

Any damage, possible compromise of information, theft/loss or inquiries on the appropriate use of Mobile Devices must be immediately reported by Fraser Health Staff to the Fraser Health Service Desk.

Device Security

- Devices must be secured according to Fraser Health standards.
- Devices accessing Fraser Health information, data and technology, managed by Fraser Health Mobile Device Management Solution, must be secured with the following security features
    - Devices must be fully encrypted in a manner that meets or exceeds the minimum requirements set out in the Information Security Policy
    - Any corporate information transmitted over the network from the corporate device must be encrypted.
    - Devices must be secured with a password and complexity that meets or exceeds the minimum requirements set out in the Fraser Health Access Control Policy.
    - Suitable antivirus/antimalware software must be properly installed and running on all personal devices as per the Fraser Health Malicious Code Standard.
    - Screen saver timeout (suspended, sleep, re-authenticate) must be set as per the Fraser Health Access Control Management standard.
    - Device operating system security must not be circumvented or modified from the manufacturers original design (jail broken/rooted) if connecting to any Fraser Health network or accessing any Fraser Health resource.
    - Attempts to circumvent the Fraser Health device security controls are prohibited.
    - Attempts to circumvent native (built-in) device security controls are prohibited.
- Fraser Health has the right to remove access to its information and applications from

users/devices that do not comply with its security standards.
- Fraser Health reserves the right to seize and forensically examine any enrolled mobile devices necessary for investigatory or control purposes. This includes turning over the device to the authorities for investigation.

Personal Devices (Bring Your Own Device)
- Personal devices are the device owner's responsibility to maintain, repair and upgrade Fraser Health only will support its applications on those devices. Fraser Health has the right to restrict applications that can be installed on the personal device if they pose a security risk to Fraser Health information or infrastructure.
- Fraser Health provided applications can only be installed via approved secure application repository/store.

Enforcement
Persons found not complying with this policy will be held accountable to actions that contravene training, agreements/oaths, policies or law. Policy breaches will be investigated in consultation with the relevant clinical and business areas (e.g., Human Resources or Legal) and are subject to disciplinary actions that can include the following:
- Suspension or termination for Fraser Health employees or volunteers;
- Contract termination for consultants/contractors and service providers;
- Loss of privileges in accordance with Medical Staff Bylaws for physicians; or
- Termination of their relationship with Fraser Health and follow-up with associated health care licensing bodies or educational institutions for contraventions by other persons acting on behalf of Fraser Health Authority (e.g., a student in a practical placement).

DEFINITIONS

Terms	Definitions
Privacy breach	The unauthorized collection, use, disclosure or disposal of personal information or personal health information that is in breach of applicable legislation/regulations, including BC Law Freedom of Information and Protection of Privacy Act (FIPPA), and/or in violation of Fraser Health policies, standards or contractual obligations.
Third party	A person or body independent of the parties involved concerning the issue in question [ISO/IEC 27002:2005].
Corporate Mobile Devices	Any Mobile Device owned and issued by Fraser Health but used to access Fraser Health information or systems.
Fraser Health Confidential	Personal Information, Proprietary Information or Other Confidential Information under the custody and/or control of Fraser Health.

POLICY TITLE **PRIVACY AND SECURITY REQUIREMENTS FOR MOBILE DEVICES**		**NUMBER** 02-774
AUTHORIZATION Vice President, Planning, Informatics and Analytics	**DATE APPROVED** November 28, 2017	**CURRENT VERSION DATE** October 19, 2017

Information	
Fraser Health Staff	All employees, volunteers, consultants/contractors, service providers, physicians, health care providers and other persons employed, engaged or otherwise acting on behalf of Fraser Health.
Mobile Devices	All readily portable devices used to process and store information. Includes, but is not limited to, laptops, notebooks, tablets, personal digital assistants (PDA) and mobile phones. Mobile Devices include Corporate Mobile Devices and Personal Mobile Devices.
Other Confidential Information	Information provided to or collected/created by Fraser Health or partner organization in the course of business operations of the Fraser Health or partner organization which may contain information about an identifiable individual. Other confidential information includes: • Information prepared as part of a pending or ongoing litigation, law enforcement investigation, internal assurance investigation, quality assurance review, coroner inquest, Workers Compensation investigation, ombudsman or human rights investigation; • Information related to credentialing, discipline, privilege, or external reviews of quality of care; • In camera deliberations of Fraser Health or a partner organization where such topics as personnel, labour relations, land acquisitions or litigation may be discussed; or • Unpublished statistical, scientific, technological, other intellectual property information, or internal correspondence related to organizational initiatives.
Personal Information	Includes any information about an identifiable individual except for business contact information. This might include a person's name, social insurance number, employment history or medical information. References to "Personal Information" within this policy apply to documents or records (hard copy or electronic form) which Personal Information is recorded and to verbal comments or conversations which personal information is mentioned or discussed.
Personal Mobile Devices	Any Mobile Device not owned and issued by Fraser Health.
Proprietary Information	Sensitive information that Fraser Health owns and is legally permitted to treat in a manner to ensure that it remains confidential. Proprietary Information includes, but is not limited to, technical, commercial and financial information.

		Page 5 of 6
POLICY TITLE **PRIVACY AND SECURITY REQUIREMENTS FOR MOBILE DEVICES**		**NUMBER** 02-774
AUTHORIZATION Vice President, Planning, Informatics and Analytics	**DATE APPROVED** November 28, 2017	**CURRENT VERSION DATE** October 19, 2017

PROCEDURE:

Roles and Responsibilities

Role	Responsibilities
Vice President of Planning, Informatics & Analytics	The Vice President of Planning, Informatics & Analytics or delegate(s) is responsible for overseeing the implementation of this policy, including monitoring compliance with the policy.
Privacy Office	The Privacy Office is responsible for managing real or suspected privacy-related incidents. The Privacy Office provides support and/or direction to the Vice President of Planning, Informatics and Analytics on privacy best practices as needed.
Staff	All Fraser Health employees (including full-time, part-time, and temporary staff), physicians, students, volunteers, business and health-care delivery partners, consultants, contractors, and service providers. Fraser Health staff is responsible for: • Complying with directives, policies, procedures and standards when using information and data assets and corporate resources included this policy; • Attending privacy and security training with respect to acceptable use of information and information systems; and • Reporting information security and privacy incidents, vulnerabilities and violations to the responsible manager (as appropriate) and the Privacy Office in accordance with Fraser Health's Managing Privacy Breaches Policy.

		Page 6 of 6
POLICY TITLE **PRIVACY AND SECURITY REQUIREMENTS FOR MOBILE DEVICES**		**NUMBER** 02-774
AUTHORIZATION Vice President, Planning, Informatics and Analytics	**DATE APPROVED** November 28, 2017	**CURRENT VERSION DATE** October 19, 2017

REFERENCES

- Freedom of Information and Protection of Privacy Act
- Protecting Personal Information Away From the Office
- https://www.oipc.bc.ca/guidance-documents/1447Fraser Health Policy – "Audit of Electronic Health Information Access"
- Fraser Health Policy – "Confidentiality and Security of Personal Information"
- Fraser Health Policy – "Electronic Communications"
- Fraser Health Policy – "Managing Privacy Breaches"
- Fraser Health Policy – "Access Control Policy"
- Fraser Health Policy – "Audit of Electronic Health Information Access Policy"
- http://www.fraserhealth.ca/airwatch