CPF0300: Information Privacy and Confidentiality Policy

Approved Date:	April 2004
Reviewed/Revised Date:	October 2013
	September 2017

1.0 Introduction

1.1 Description

Providence Health Care (PHC) has value-based, ethical, and legal obligations to protect Personal Information about its patients, residents and Staff. It may also be obliged under contract or other circumstances to protect Confidential Information.

The purpose of this Information Privacy & Confidentiality Policy ("Policy") is to establish the guiding principles and framework by which PHC and its Staff will comply with these obligations, demonstrate accountability for managing Personal Information and Confidential Information and maintain its trust-based relationship with patients, residents, Staff, business and healthcare partners (including Lower Mainland Consolidation parties) and the public.

1.2 Scope

This Policy applies to all Staff relating to Personal and Confidential Information regardless of format or how it is stored or recorded.

For the purposes of this Policy, Staff is defined as all officers, directors, employees, physicians, dentists, midwives, nurse practitioners, residents, fellows, health care professionals, students, volunteers, researchers, contractors and other service providers engaged by PHC.

2.0 Policy

Policy statement

PHC and its Staff will comply with the BC Freedom of Information and Protection of Privacy Act (FIPPA), the Personal Health Information Access and Protection of Privacy Act (e-Health Act) and other legislation, professional codes of ethics and standards of practice.

All Staff must ensure that their practices in collecting, accessing, using or disclosing Personal Information and Confidential Information comply with this Policy as well as with other applicable laws, professional codes of practice and contractual obligations. These obligations for ensuring privacy and confidentiality continue after the employment, contract or other affiliation between PHC and its Staff comes to an end.

2.1 Confidentiality Undertaking

As a condition of employment or affiliation, all Staff must read the Information Privacy and Confidentiality Policy and acknowledge their understanding of their privacy obligations by signing an approved Confidentiality Undertaking (see Appendix I) or other agreement as deemed applicable by PHC. All Staff will be required to re-affirm their understanding of and commitments to upholding confidentially on a regular basis as determined by PHC.

2.2 Privacy Education

Staff must complete mandatory privacy education as determined by PHC. Privacy education will be determined based on the Staff roles and responsibilities at PHC.

2.3 Collection of Personal Information

Staff may collect Personal Information as needed to operate PHC programs or activities and will not collect more Personal Information than is required to fulfill those purposes.

Direct Collection:

Where possible, Personal Information will be collected directly from the individual the information is about. At the time of collection, the individual should be informed of:

- the purpose for the collection
- the legal authority for the collection; and
- the contact person if the individual has any questions about the collection.

PHC informs the individual through the "Caring for Your Information – Notice to our Patients and Residents" sign. These signs will be posted at all registration, intake and admission sites, including community clinics.

Indirect Collection:

In circumstances where it is not possible or practical to collect information directly from an individual and where it is not possible to obtain consent for another method of collection; PHC can indirectly collect Personal Information as authorized including:

- when the information is necessary to provide medical treatment
- when the information is necessary to facilitate ongoing medical treatment, it may be collected from or shared with other Health Authorities or health care providers.

2.4 Use of Personal Information

Staff may access, and use Personal Information for legitimate purposes based on a "need to know" in order to perform job functions and responsibilities.

Primary Use

PHC primarily collects Personal Information for providing health care services to patients and residents. Staff may use Personal Information for the provision of care and for administrative and other support functions related to direct care.

Secondary Use:

Staff may use Personal Information for purposes related to the provision of care ("Secondary Purposes") only if the purpose has a reasonable and direct connection to the provision of health care services and is required for an operating program of PHC. For example:

- Program evaluation and monitoring, including quality improvement;
- System administration;
- Privacy and security audits; and
- Medical education and training related to PHC programs.

As a general rule, Staff should limit the amount of Personal Information used for a Secondary Purpose to only that which is necessary to achieve the purpose. Where possible, personal identifiers (e.g. name, birth date, PHN, MRN, home address, postal code, personal phone number, SIN, employee ID number, etc.) should be removed from records and documents, such as statistical management reports or sample electronic health records used for system training.

Secondary Use for Research: Refer to section 2.5.

2.5 Disclosure of Personal Information

The following are examples where Personal Information may be disclosed. Staff may consult with the Information Access and Privacy Office for questions about disclosure.

Disclosure or Sharing for Continuity of Care:

Staff may share or disclose Personal Information on a "need to know" basis to other health care providers or members of the care team for continuity of care purposes.

Disclosure for Safety Purposes:

Staff may, without requiring consent, disclose Personal Information necessary to provide warning or to avert a risk:

- Where compelling circumstances exist affecting the health or safety of any individual; or
- To protect the public in circumstances where there is a risk of significant harm to the environment or to the health or safety of the public or a group of people

Good-faith Decision-making

PHC will not dismiss, suspend, demote, discipline or otherwise disadvantage a Staff member who, acting in good faith and upon a reasonable belief, discloses Personal Information necessary to provide warning or to avert risk where immediate action is required to prevent harm to any person's health or safety.

Disclosures to Law Enforcement

For disclosures of Personal Information to law enforcement (e.g. mandatory demands such as court orders or search warrants, requests by law enforcement, or PHC-initiated reporting to law enforcement), refer to *Policy CPF1700: Release of Personal Information and Belongings to Law Enforcement Agencies*.

Disclosure Outside of Canada:

Staff will not access, transfer or store Personal Information outside of Canada, except with the consent of the individual or as otherwise permitted by FIPPA (e.g. for temporary access for systems support). Staff will consult with the Information Access and Privacy Office prior to implementing any program or other initiative in which Personal Information will be transferred, stored or accessed outside of Canada.

Requirements before disclosing or allowing access to Personal Information to Third Parties:

Where Personal Information is shared with, accessed or stored by a third party vendor, contractor, agency or other organization; a written agreement or other legal documentation may be required. Staff must consult with the PHC Information Access and Privacy Office to determine what documentation is required.

Examples where legal documentation may be required are as follows:

- Access by a third party organization to a PHC clinical information system;
- Services provided by a vendor who will have access to Personal Information; or
- A program that requires Personal Information to be shared with another organization.

Disclosure for Research Purposes:

The disclosure of Personal Information to Staff or third parties for research must be done in accordance with Section 35 of FIPPA and have Research Ethics Board approval. Access to Personal Information may

require the execution of an information sharing agreement and must also adhere to applicable PHC and IMITS policies, system access requirements and procedures.

Disclosure for Fundraising Purposes:

Personal information can only be shared with Hospital Foundations if explicit consent has been obtained. Foundations are considered to be separate organizations from the corporation and fundraising is not a consistent purpose with normal collection of Personal Information.

2.6 Accuracy of Personal Information and Handling Requests for Correction of Personal Information

PHC and its Staff will take all reasonable steps to ensure the accuracy and completeness of any Personal Information they collect or record and be diligent to protect against making any errors due to carelessness or other oversights.

Health Information Management (Health Records) is responsible for updating and maintaining the accuracy of health records. Staff should direct any patients or residents requesting correction or amendment of information in their medical records to Health Information Management.

2.7 Retention and Destruction of Personal Information

PHC must retain records containing Personal Information for a minimum of one year if the Personal Information is used to make a decision that directly affects the individual the information is about. Records will be retained in accordance with any ministerial directives and all legal, regulatory and accreditation requirements, as well as with any PHC record retention policies.

When Personal Information is to be destroyed, Staff will follow the PHC guidelines and procedures for the secure destruction of Personal Information to ensure the information is destroyed, erased or made anonymous.

2.8 Protecting Information

Staff must take “reasonable security precautions” to ensure that all Personal Information and Confidential Information is protected against unauthorized access, collection, use, disclosure, or disposal. Staff are expected to be familiar with, maintain and enforce the physical and technical security measures applicable to their own program areas and must be aware of and adhere to applicable policies, including IMITS Policies as well as any guidelines for protection of personal information.

2.9 Reporting Privacy Breaches

Staff must immediately report any actual or suspected privacy breaches or violations of this Policy, including the theft or loss of Personal Information, devices or paper records, to the Information Access

and Privacy Office. Privacy breaches will be dealt with in accordance with the Managing Privacy Breaches Policy.

If Staff wishes to report anonymously, they can follow the process set out in the CPF1500: Safe Reporting Policy.

2.10 Privacy Impact Assessment

A Privacy Impact Assessment (PIA) must be completed before implementing or significantly changing any program or system that involves collection, use, disclosure or storage of Personal Information.

PHC departments should contact the Information Access & Privacy Office who will determine if a PIA is required and will support the process. Completion of a PIA and addressing any compliance gaps identified in the PIA is the responsibility of the department leading the change or initiative.

2.11 Release of Information Requests

Health Records:

- Staff may provide patients/residents with a copy of a document if it was completed with the patient/resident present (e.g. patient assessment, care plan). Staff may also provide patient/resident with a copy of a single lab or radiology report if they request. Staff will document the release of the record in the patient chart.
- Patients/residents requesting a copy of their entire health record or health records narrative in nature (e.g. progress notes, transcribed reports), should direct their request to Health Information Management (Health Records Department).

Employee Information – Refer requests for employee information from legal firms, financial institutions, insurance companies, credit bureaus, etc. to Human Resources.

Corporate/Non-Health Records: Refer requests to the Information Access and Privacy Office.

2.12 Compliance Monitoring and Auditing

Compliance to this Policy will be monitored and all suspected breaches will be investigated by the Information Access and Privacy Office. Actions to be taken will be determined by Human Resources, Office of the General Counsel, and/or other PHC stakeholders according to the nature of the breach and parties involved.

PHC operational areas and programs must conduct appropriate reviews and audits of their systems and processes to ensure compliance in accordance with PHC and IMITS policies and standards.

2.13 Reporting Privacy Breaches

Staff must immediately report any actual or suspected breaches of privacy, including the theft, loss or attempted theft of Personal Information or devices on which Personal Information may be stored. Privacy breaches shall be dealt with in accordance with PHC Policy: CPF1600: Managing Privacy Breaches.

2.14 Challenging PHC's Compliance to Policy

Providence Health Care, through the Information Access and Privacy Office will investigate all complaints from individuals concerning compliance with this Policy. If the complaint is found to be justified, appropriate measures will be taken, including amending policies and procedures where required. The individual will be informed of the outcome of the investigation.

2.15 Compliance

Failure to comply with this Policy may result in disciplinary action including, but not limited to, the termination of employment, loss of computing privileges, loss of privileges as a student placement or volunteer role, prosecution and restitution for damages.

3.0 Procedure

3.1 Responsibilities

Accountability for PHC compliance with this Policy rests with the Vice President Human Resources and General Counsel. The Leader, Information Access & Privacy is responsible for oversight and compliance with this Policy and other Staff within PHC are responsible for day-to-day collection, processing and protection of Personal Information.

3.1.1 Information Access and Privacy Office (IAPO)

- General oversight of privacy practices within PHC and maintenance of breach and compliance policies;
- Providing privacy education to Staff and promoting good privacy practices throughout the organization;
- Responding to questions from Staff, Patients/Residents and members of the public concerning collection, access, use and disclosure of Personal Information;
- Investigating potential and actual breaches of this Policy brought to its attention and reporting breaches in accordance with PHC breach policies;
- Supporting Health Information Management and other Programs on Release of Information issues;
- Supporting the completion of Privacy Impact Assessments;
- Managing Freedom of Information (FOI) requests; and

- Acting as the point of contact for the Office of the Information and Privacy Commissioner of British Columbia (OIPC) when complaints are received about PHC's compliance with FIPPA;

3.1.2 Leaders/Managers

- Overseeing compliance with this Policy by Staff within their area(s) of responsibility

3.1.3 Staff

- Ensuring that appropriate steps are taken to protect Personal Information and Confidential Information at all times;
- Ensuring that access to and disclosure of Personal Information or Confidential Information is only made by or to authorized individuals;
- Complying with the IMITS policies and security requirements developed for the use of electronic systems; and
- Reporting to the Information Access and Privacy Office any actual or suspected breaches of privacy or of this Policy and cooperate with any related investigations.

The obligations for ensuring privacy and confidentiality set out in this policy continue after the employment, contract or other affiliation between PHC and its Staff ends.

4.0 Supporting Documents and References

4.1 Related Policies

CPF1700: Release of Information and Belongings to Law Enforcement
CPF1500: Safe Reporting Policy
CPF1600: Managing Privacy Breaches

4.2 Related Standards / Forms / Guidelines

Confidentiality Undertaking

4.3 Definitions

"Confidential Information" means all information, other than personal information, that is specifically identified as confidential or is reasonably understood to be of a confidential nature that Staff receive or have access to through PHC or other Lower Mainland consolidation parties, including vendor contracts and other proprietary information that a Lower Mainland Consolidation party may have received from a third party.

"FIPPA" means the *BC Freedom of Information and Protection of Privacy Act*, as amended from time to time.

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

"IAPO" means Information Access and Privacy Office for Providence Health Care.

"IMITS" means the consolidated Information Management/Information Technology Services department of Provincial Health Services Authority, Providence Health Care, and Vancouver Coastal Health Authority.

"Lower Mainland Consolidation" means the consolidation of certain corporate and clinical support functions amongst Vancouver Coastal Health authority, Fraser Health Authority, Provincial Health Services Authority and Providence Health Care Society as more fully set out in a Master Services Agreement amongst the parties dated January 1, 2011.

"Patients and Residents" mean all people receiving services from PHC. For ease of language, Clients and Assisted Living tenants are not specifically named but are implied in any reference to patient/resident.

"Personal Information" means any information about an identifiable individual but does not include business contact information, such as a person's title, business telephone number, business address, email or fax number.

"Privacy Impact Assessment" (PIA) means the assessment of a current or proposed initiative (a system, project, program, or activity) to evaluate privacy impacts, including evaluating compliance with this Policy and with PHC's privacy responsibilities under FIPPA.

"Reasonable Security Precautions" means those that a fair, rational person would think were appropriate to the sensitivity of the information and to the medium in which is stored, transmitted, handled or transferred. A sliding scale of security arrangements is appropriate, depending on the sensitivity of the personal information that an organization handles.

"Staff" means all officers, directors, employees, physicians, dentists, midwives, nurse practitioners, residents, fellows, health care professionals, students, volunteers, researchers, contractors and other service providers engaged by PHC.

4.4 References

BC Freedom of Information and Protection of Privacy Act (FIPPA) [RSBC 1996] Chapter 165

4.5 Keywords

Confidentiality, privacy, undertaking, collection, use, disclosure, sharing, storing, retention, access, audit, compliance, breach, retention, research, secondary purpose

4.6 Questions

Contact: Information Access and Privacy Office (IAPO) at privacy@providencehealth.bc.ca