CPF0300: Information Privacy and Confidentiality Policy

Approved Date: April 2004

Reviewed/Revised Date: October 2013

1.0 Introduction

Description

Providence Health Care (PHC) has value-based, ethical, and legal obligations to protect Personal Information about its patients, residents and Staff.

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 its obligations regarding the protection and management of Personal Information and other Confidential Business Information under the custody and control of PHC. It also applies to information under the custody and control of any other Health Organization that PHC provides services and to which PHC employees have access to while performing their role, such as services provided through Lower Mainland Consolidation.

Scope

This policy applies to all Staff relating to Personal and Confidential Business Information regardless of format or how it is stored or recorded. This policy applies while in the course of working and conducting business for or on behalf of PHC, including when off-duty, and extends beyond the completion of the employment or business relationship.

2.0 Definitions

For purposes of this policy:

"Confidential Business Information" means any Corporate-related, financial or administrative information. This includes information stored on all forms of media including, but not limited to, paper, electronic, magnetic, optical disk and microfiche.

"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, 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.

3.0 Policy

3.1 Privacy Legislation and Policies

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 Business Information comply with this Policy as well as with other applicable statutory requirements, 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.

3.2 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.

3.3 Privacy Training

Staff must complete Privacy Training as determined by PHC. Privacy training will be determined based on the Staff roles and responsibilities at PHC.

3.4 Collection of Personal Information

PHC complies with FIPPA in regards to the collection of Personal Information. Collection must be **limited** to only what is needed to fulfill the purposes identified.

Purpose for Collection**:**
Staff must only collect Personal Information for the following purposes:

- a purpose directly related to and necessary for delivering a program or activity of PHC (e.g. the delivery of health care services; or for managing the employment relationship);
- where the information is necessary for the purposes of planning or evaluating a program or activity of PHC; or
- where the collection is otherwise authorized by legislation.

Informing the Individual**:**
At or before the time Personal Information is collected, individuals should be informed of the purpose for which the information is being collected and the authorization for doing so and who to contact if the individual has any questions. PHC posts notification signs (Caring for Your Information – Notice to our Patients and Residents) at all intake and registration areas.

Direct Collection:
Where possible, Personal Information will be collected directly from the individual the information is about.

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 and it is not possible or practical to collect the information from the patient/resident or to obtain consent, then Staff may collect Personal Information from others, such as friends or family members; or
- 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.

3.5 Use of Personal Information

All access to and use of Personal Information by Staff must be exercised on a "need to know" basis and for purposes that are necessary for the performance of an individual's job functions and responsibilities.

Staff must only access and use Personal Information for the following purposes, as authorized by FIPPA:

- The purpose(s) for which the information was originally collected by PHC, such as for health care delivery or administrative and other support functions related to provision of care; or for management of employment;
- For a purpose for which the individual has provided explicit consent; or
- The purpose(s) for which the information was disclosed to PHC by another Health Organization.

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;
- 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, postal codes, SIN, employee ID number, etc.) should be removed from records and documents.

3.6 Disclosure of Personal Information

Under FIPPA, disclosure occurs whenever Personal Information is provided to or accessed by someone.

Internal Disclosure or Sharing:
Staff may only share or disclose Personal Information on a "need to know" basis to other Staff, if those persons require the information in order to perform their job functions.

Disclosure to External Parties – General Requirements:
The disclosure of Personal Information to persons or parties other than Staff must be made only where such disclosure is permitted by FIPPA and authorized by PHC. PHC is authorized to disclose Personal Information in the following circumstances:

- For the purpose for which it was obtained or compiled or for a use consistent with that purpose (e.g. continuity of care);
- Where the individual explicitly consents to the information being disclosed;
- To a service provider for PHC where the service provider is obligated by legal agreement to abide by FIPPA, and the conditions under "Sharing Personal Information with Third Parties" are met (see requirements below);
- *Where specifically required or authorized by law (e.g. by legislation, court order, subpoena or warrant)
- *Where compelling circumstances exist affecting the health or safety of any individual;
- *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.

*For disclosures to Law Enforcement Agencies - refer to *Policy CPF1700: Release of Personal Information and Belongings to Law Enforcement Agencies*

Disclosure Outside of Canada:
All Staff must ensure that no Personal Information is accessed, transferred or stored outside of Canada, except with the explicit consent of the individual the information is about or as otherwise permitted by FIPPA, such as to collect a debt owing to PHC or to contact an individual's next of kin in an emergency.

Staff must 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.

Staff should take all reasonable steps to ensure no unauthorized personnel or third parties are provided with access to records containing Personal Information. Any third party who requests access should be asked to produce identification and confirmation that they have signed an agreement in accordance with this policy.

Personal information may also be shared in limited circumstances between PHC and another public body or ministry for specific integrated programs. Consult with the Information Access & Privacy Office prior to any disclosures of Personal Information in this circumstance.

Disclosure for Research Purposes:
The disclosure of Personal Information for research purposes 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.

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

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.

An individual who believes that there is an error on his or her Personal Information may request correction of this information. PHC Departments in control of the Personal Information at issue must

consider any request to correct the Personal Information. Where the individual successfully demonstrates that the Personal Information is inaccurate, the record must be corrected. If no correction or addition is made, the record must be annotated with the correction that was requested but not made.

3.8 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 all legal, regulatory and accreditation requirements, as well as with any PHC record retention policies. Currently, PHC retains health records for longer periods to comply with Ministry of Health directives.

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.

3.9 Protecting Information

Staff must take "reasonable security precautions" to ensure that all Personal Information and Confidential Business Information is at all times protected against unauthorized access, use, collection, disclosure, storage, retention, duplication, loss, theft and 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.

3.10 Reporting Breach of Policy

Staff must immediately report any actual or suspected violation of this Policy to the Information Access and Privacy Office. If Staff wishes to report anonymously, they can follow the process set out in the CPF1500: Safe Reporting Policy.

3.11 Privacy Impact Assessment (PIA)

PHC departments must complete a PIA prior to making a significant change to a current program/system or when undertaking any new initiative, program or activity that involves Personal Information. Completion of a PIA and addressing the compliance gaps identified in the PIA is the responsibility of the department leading the change or initiative.

Contact the Information Access and Privacy Office early in the planning process to avoid any delay in implementing. The IAPO will determine if a PIA is required and will then provide advice and support to assist in the completion of the PIA.

3.12 Responding to Access Requests from the Public, Patients/Residents, Staff and Governmental Authorities

Under FIPPA, members of the public have the right to request access to records within the custody or control of public bodies. Individuals also have the right to access their own information, including medical information.

Staff members receiving access requests should refer the requests to the appropriate department, as follows:

- Health Records – Requests for health records for provision of care purposes and in response to patients/residents (or their authorized or legal representative) for their medical information should be referred to the Health Records Department.
- Employee Information – requests for information on other staff members should be directed to Human Resources.
- Employment Files – Requests for access to employment, payroll or human resources files received from employees, legal firms, financial institutions, insurance companies, credit bureaus, the Canada Revenue Agency and police should be directed to Human Resources.
- Non-Medical Records – Formal requests under Part 2 of FIPPA for access to non-clinical records should be directed to the Information Access and Privacy Office.

3.13 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.

3.14 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.

3.15 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.

4 Responsibilities

4.1 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.

4.2 The Information Access and Privacy Office (IAPO) is responsible for:

- 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;

4.3 Leaders/Managers are responsible for:

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

4.4 Staff are responsible for:

- ensuring that appropriate steps are taken to protect Personal Information and Confidential Business Information at all times;
- ensure that access to and disclosure of Personal Information or Confidential Business 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.

4.5 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.

5 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.

6 References

References

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

Tools, Forms and Guidelines

- Confidentiality Undertaking

Related Policies

- CPF1700: Release of Information and Belongings to Law Enforcement
- CPF1500: Safe Reporting Policy
- CPF1600: Managing Privacy Breaches
- CPF2200: Out-patient Requests for Health Records

Keywords

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