CPF0300: Information Privacy & Confidentiality Policy

Approved Date: April 2004
Revised Dates: Feb 2011; Nov 2012

1.0 PURPOSE

Providence Health Care (PHC) has value-based and ethical obligations, as well as legal obligations under *BC Freedom of Information and Protection of Privacy Act (*"*FIPPA")*, the *Health Act*, and other legislation and standards of practice, for the control or custody of Personal Information about its patients, residents and Staff.

The purpose of this Information Privacy & Confidentiality Policy ("Policy") is to provide consistent standards to ensure that employees of PHC are aware of and acknowledge these obligations to protect the personal information and other confidential information under the custody and control of PHC or under the custody and control of any other Health Authority that PHC provides services to and to which PHC employees have access to while performing their role.

2.0 SCOPE

This policy applies to all PHC Staff and all Personal and Confidential 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

3.0 DEFINITIONS

"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.

"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 (including, but not limited to patients, residents, volunteers, students, Staff, physicians or members of the public), but it does not include business contact information (business contact information is information such as a person's title, business telephone number, business address, email or facsimile number).

Examples of Personal Information include but are not limited to:

- The individual's name, address, telephone number, personal healthcare number;
- An individual's race, national or ethnic origin, colour or religious beliefs or associations;
- An individual's age, sex, sexual orientation, marital status or family status;
- 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 an individual's educational, financial, criminal or employment history;
- Anyone else's opinions about the individual;
- 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.

"Privacy Impact Assessment" means the process to determine whether new systems, programs, initiatives, strategies or proposals meet the privacy and security requirements of the *BC Freedom of Information and Protection of Information Act*, other regulatory requirements and PHC policies and principles for information privacy and confidentiality.

"Staff" means all officers, directors, employees, contractors, physicians, dentists, midwives, health care professionals, students and volunteers engaged by PHC.

4.0 POLICY

4.1 Accountabilities

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

Leaders/Managers
Management Staff have a responsibility to oversee compliance with this Policy by Staff within their area(s) of responsibility.

Staff
All members of Staff have responsibility to ensure that appropriate steps are taken to protect Personal Information at all times. They must ensure that their practices in collecting, accessing, using or disclosing Personal Information comply with this Policy as well as with statutory requirements and their professional codes of practice. In addition, Staff are expected to report to the PHC Information Access & Privacy Office any concerns with or recommended improvements to information privacy and security procedures, and any information to help resolve problems.

4.2 Acknowledgement of Confidentiality

PHC will make all Staff aware of the importance of maintaining the confidentiality of Personal Information and other confidential business information. As a condition of employment or affiliation, all new Staff must read the Information Privacy and Confidentiality Policy and sign an approved Confidentiality Acknowledgement (see Appendix I). In addition, personal information obtained in the course of one's employment or other affiliation with PHC must be held in confidence even after the affiliation comes to an end.

4.3 Failure to Comply

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.

4.4 Collection of Personal Information

The collection of Personal Information by PHC is governed by FIPPA and must be limited to what is needed to fulfill the purposes identified.
At or before the time Personal Information is collected, Staff must provide notification and information material to patients and residents at all registration, intake and admission sites advising them of:

- the purpose for which the information is being collected and the authorization for doing so,
- how it will be used by PHC and its Staff, and
- who to contact if the client has any questions about the collection and use.

Staff may only collect and use Personal Information for purposes:

- directly related to an operating program or activity of PHC (i.e. the delivery of health care services or for administration or employment purposes), or,
- where the individual has explicitly consented to the use of their information, or
- where collection is authorized by FIPPA, or,
- otherwise by law.

Where possible, Staff shall collect Personal Information directly from the client to whom it relates unless the individual agrees or there is some legal authority for using an indirect method of collection. In circumstances where it is not possible or practical to collect information or obtain consent directly from the individual, then Staff may collect Personal Information indirectly from other sources authorized by FIPPA. For example:

- Information necessary to facilitate medical treatment may be collected from friends or family members;
- Information necessary to facilitate ongoing medical treatment may be collected or shared with other Health Authorities or health care providers; or
- Information may be collected indirectly for the purposes of law enforcement or if Staff are authorized by other legislation to collect such information.

4.5 Accuracy of Personal Information

Staff must 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.

4.6 Access, Use, Disclosure or Sharing of Personal Information

Staff is only authorized to access, use, disclose or share Personal Information for legitimate purposes based on a “need to know” basis in order to perform their job functions and responsibilities.

No Staff may release personal information about a patient, resident or other employee except in limited circumstances authorized under FIPPA legislation. These circumstances include:

- Where prescribed by law (including legislation, court order, subpoena or warrant) - Refer to *Policy CPF1700: Release of Personal Information/Belongings to Police and Other Law Enforcement Agencies* and *Policy CPF1800: Receipt & Disposition of Legal Documents Served at Providence Health Care*.
- Where compelling circumstances affect the health or safety of any person or the public;
- In order 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 group of people.

Personal information may also be shared in limited circumstances between PHC and another public body or ministry for specific integrated programs. The Information Access and Privacy Office must be consulted prior to the disclosure of Personal Information in this circumstance.

Personal information may also be shared in limited circumstances for research purposes where legislative conditions have been met. The Research Ethics Board must approve all research projects prior to disclosure of Personal Information.

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.

4.7 Release of Information

Staff are expected to comply with all PHC policies, procedures and guidelines for the release of Personal Information on patients, residents and other staff members and ensure all releases comply with FIPPA and other applicable legislation.

4.8 Accessing or Sharing Personal Information with Third Parties

Before Personal Information in the custody or control of PHC is accessed by or shared with a contractor or other third party organization, and where explicit patient consent has not been obtained, both parties must execute an information access agreement, information sharing agreement and/or privacy schedule. The Leader, Information Access and Privacy or General Counsel must approve the form of all information access agreements, information sharing agreements and privacy schedules.

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.

Staff are responsible for ensuring that no Personal Information is accessed, transferred or stored outside of Canada except with the consent of the individual the information is about, or where otherwise permitted by FIPPA legislation. The Information Access and Privacy Office must be consulted before any program is implemented in which Personal Information will be transmitted, transported or stored outside of Canada.

4.9 Security of Information

PHC is committed to maintaining the security of Personal Information and other sensitive information, including appropriate physical security of records and security safeguards for computer and network systems. Staff are expected to comply with PHC security requirements developed for use of such systems.

All Staff have the responsibility to protect against unauthorized access and disclosure of Personal Information. This responsibility includes ensuring that access or disclosure is only made to or by authorized individuals and reasonable measures are taken to prevent any unauthorized access, disclosure, loss or theft of information.

4.10 Retention and Destruction of Personal Information

Records will be retained in accordance with all legal, regulatory and accreditation requirements, as well as with any PHC record retention policies. Staff holding records containing Personal Information are expected to identify retention times and then follow the PHC guidelines and procedures for the secure destruction of Personal Information that is no longer required to ensure the information is destroyed, erased or made anonymous.

4.11 Privacy Impact Assessment

A Privacy Impact Assessment ("PIA") must be completed before implementing or significantly changing any program or system that requires the collection, use, disclosure or sharing of Personal Information. Contact the Information Access & Privacy Office to determine whether a PIA is required. Completion of a PIA is the responsibility of the department responsible for the new service or delivery, with support from the Information Access & Privacy Office.

4.12 Compliance Monitoring, Auditing & Consequences

Access, use, disclosure and sharing of Personal Information will be monitored and all suspected breaches of this Policy will be investigated by the Information Access and Privacy Office. Actions to be taken will be determined by Human Resources, Legal Services 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 with PHC policies and standards.

4.13 Breach of Policy

Staff are expected to report any real or suspected breaches of this Policy in connection with any PHC program or activity. All reports must be made to the Information Access and Privacy Office. Staff may report real or suspected breaches without any fear of reprisal. Such reports will be covered by the PHC policy that protects "whistle blowers" (CPF1500 *Protection of Staff Who Report Financial Improprieties or Other Misconduct*).

All incidents involving theft or loss of Personal Information will be promptly addressed for containment, investigation, reporting, and remedial actions.

4.14 Openness

PHC will make available, directly to individuals, specific and easy to understand information about its policies and practices related to the management of Personal Information. PHC will include:

- the title and address of the person or persons accountable for PHC compliance with this Policy and to whom inquiries or complaints can be directed;
- the available means of gaining access to Personal Information held by PHC; and
- a description of the type of Personal Information held by PHC, including a general account of its use.

4.15 Challenging Compliance

PHC will maintain procedures for addressing and responding to all inquiries or complaints from individuals about its handling of Personal Information and will inform its patients and residents about the existence of these procedures.

An individual will be able to challenge compliance with this Policy with the Information Access and Privacy Office to ensure the issue is properly discussed, documented and addressed as quickly as possible. All complaints will be investigated, and, if 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.

5.0 PROCEDURES

5.1 General Inquiries or Requests to Amend Personal Information

Questions or concerns about collection, access, use or disclosure of Personal Information, reports of privacy breaches or loss of information should be directed to the Information Access and Privacy Office (604 806-8336).

Staff should direct any patients or residents requesting correction or amendment of Personal Information in their medical records to the Health Record Services.

5.2 Complaints

Patients, residents or other members of the public who complain about a breach of their personal privacy or who express concern about the collection or use of their Personal Information should be directed to the Information Access and Privacy Office or the PHC Client Relations Department.

5.3 Requests for Information

Clinical Information
Any questions or concerns about the release of clinical information should be directed to Health Record Services. This includes requests by patients, residents, family members, friends, and any other third party. (Note: Requests for clinical information specific to one service/department (e.g. lab) may be made directly to and managed by that dept.)

Employee Information
Staff will direct all requests for information on other staff members to Human Resources. This includes requests from any persons (e.g. family members, friends), legal firms, financial institutions, insurance companies, credit bureaus and police, etc. This information may be provided upon receipt of the employee's written authorization, but Human Resources may confirm dates of employment without written authorization.

Employees wishing to view their employment records must submit a written request to Human Resources.

Patient's Request for Access to their Own Health Record
Patients have a right to access the information contained in their medical record and PHC will facilitate the process, as follows:

If the patient is an outpatient or has been discharged, refer them to Health Record Services.

If the patient is in a Providence Health Care facility, access will be provided as long as it doesn't interfere with the patient's own care. Arrange a convenient time when an appropriate employee is available to review the record with the patient. The employee's role is to answer any questions and to protect the integrity of the Health Record.

Only in the following rare circumstances will immediate access be denied:

- If in the physician's opinion, viewing the contents at this time would adversely affect the patient's course of treatment or would potentially harm the patient or another individual.
- If the Health Record contains Personal Information about others which was not provided by the patient (third party information). Alternatively, the section containing the third party information may be removed from the Health Record before allowing the patient access.

If access is not permitted, inform the patient that they may make a written request to Health Record Services for a copy of their Health Record upon discharge.

Other requests for information are directed to the appropriate department or agency.

Requests made:	**Refer to:**
By researchers or other individuals for research or statistical purposes	Health Record Services
By the media	Communications
For medical staff information	Medical Affairs
For litigation purposes	Risk Management & Patient Safety
By WCB, ICBC	Health Record Services
For adoption information	Health Record Services
Other FOI requests	Information Access & Privacy Office

5.4 Confidentiality Acknowledgements

The responsibilities for obtaining and holding confidentiality Acknowledgements for all new Staff are as follows:

Staff type:	**Department Responsible**
Employees	Human Resources
Students	Department responsible
Medical Staff	Medical Affairs
Volunteers	Volunteer Office

5.5 Reporting a Breach

If an intentional or inadvertent privacy breach occurs, refer to *Policy CPF1600: Managing Privacy Breaches*.

6.0 EXCEPTIONS

There are no exceptions to this policy.

7.0 FORMS/TOOLS

Confidentiality Acknowledgement

Privacy Schedule

Information Sharing Agreements (under review)

Client Brochure: Privacy and Freedom of Information: what you should know about the collection, use and sharing of personal information.

Client Poster: What you should know about the collection of your personal information

8.0 RELATED POLICIES

CPF1500: Protection of Staff Who Report Financial Improprieties or Other Misconduct

CPF1600: Managing Privacy Breaches

CPF1700: Release of Personal Information/Belongings to Police and Other Law Enforcement Agencies

CPF1800: Receipt & Disposition of Legal Documents.

9.0 REFERENCES

BC Freedom of Information and Protection of Privacy Act (FIPPA)

Canadian Standards Association (CSA) Model Code for the Protection of Personal Information

10.0 APPENDICES

Appendix I: Confidentiality Acknowledgement

Appendix II: Information Privacy & Confidentiality Policy – excerpts from CFP0300

Providence HEALTH CARE
How you want to be treated.

Confidentiality Undertaking

For PHC Employees (General)

In consideration of my employment at Providence Health Care ("PHC"), I acknowledge and agree as follows:

- I have read, understand and will adhere to the PHC Information Privacy & Confidentiality policy (link below) and related policies as amended from time to time, concerning the collection, use and disclosure of "Personal Information", as defined in the BC *Freedom of Information and Protection of Privacy Act*, obtained in the course of my employment with or provision of services to PHC;
- I understand that all Personal Information concerning staff and clients who receive services (including medical records relating to patients and residents) is confidential and may not be communicated to anyone in any manner, except as authorized by PHC, or applicable policies;
- I understand and acknowledge that all information regarding PHC, including corporate, financial and administrative records, is confidential and may not be communicated or released to anyone in any manner except as authorized by PHC, or applicable policies;
- I understand I must protect all confidential information taken outside the office from theft or loss. This includes keeping the information with me at all times, storing it in a locked and secured area when unattended, and encrypting and password protecting it when stored on electronic mobile devices (e.g. USB drives, laptops, etc.);
- I will not copy, alter, interfere with, destroy or remove any confidential information or records except as authorized by PHC in accordance with established policies;
- I understand that access to patient care information systems and other records is only for the purpose of and limited to what is required to perform my role. I will not access my record or those of family, friends or others, unless I am directly involved in providing care or other services to the individual the information is about;
- I will immediately report to my Information Privacy Office the potential or actual unauthorized disclosure or loss of any Personal Information as per policy;
- I understand that compliance with this Undertaking is a condition of my employment or service contract with PHC and that failure to comply may result in immediate termination of my employment or services, in addition to legal action by PHC and/or others.

By accepting these terms, I am confirming that I acknowledge, understand and agree to the above.

☐ I accept these terms. *(please tick the box)*

Name (please print)	Signature	Employee No.	Date

CPF0300: PHC Information Privacy & Confidentiality Policy can be found on PHCConnect at:
http://phcmanuals.phcnet.ca/corporate/doc/CPF0300.asp?LibCode=CORP

Information Privacy & Confidentiality Policy – Excerpts from CPF0300

Providence Health Care (PHC) and its Staff comply with the *BC Freedom of Information and Protection of Privacy Act ("FIPPA"),* the *Health Act* and other legislation, professional codes of ethics and standards of practice. PHC is committed to ensuring that individual privacy rights are respected. Where consistent with its statutory obligations, PHC also applies the principles set out in the *Canadian Standards Association (CSA) Privacy Code for the Protection of Personal Information.*

Assuring patients and residents that their information will be kept confidential is essential to the establishment of a trust-based relationship, which improves the quality of care because patients and residents will provide better and more complete information for decisions made with care providers.

Accountability - All members of Staff have responsibility to ensure that appropriate steps are taken to protect Personal Information at all times. They must ensure that their practices in collecting, accessing, using or disclosing Personal Information comply with the Information Privacy & Confidentiality Policy as well as with statutory requirements and their professional codes of practice. PHC will make all Staff aware of the importance of maintaining the confidentiality of Personal Information and other confidential business information. As a condition of employment or affiliation, all new Staff must read the Information Privacy and Confidentiality Policy and sign an approved Confidentiality Acknowledgement.

Compliance - Failure to comply with the Information Privacy & Confidentiality 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.

Collection - The collection of Personal Information by PHC is governed by the BC "FIPPA". Staff must provide notification and information material to patients and residents at or before the time Personal Information is collected, limit collection to what is needed to fulfill the purposes identified, and may only use the Personal Information as it directly relates to an operating program or activity of PHC or as authorized by law.

Accuracy - Staff must 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.

Access, Use, Disclosure or Sharing of Personal Information - Staff is only authorized to access, use, disclose or share Personal Information for legitimate purposes based on a "need to know" basis in order to perform their job functions and responsibilities.

Release of Information - Staff are expected to comply with all PHC policies, procedures and guidelines for the release of Personal Information. Release of health record information will also comply with FIPPA and other applicable legislation.

Accessing or Sharing Personal Information with Third Parties - Staff should take all reasonable steps to ensure no unauthorized personnel or third parties are provided with access to records containing Personal Information. Staff are responsible for ensuring that no Personal Information is accessed, transferred or stored outside of Canada except with the consent of the individual the information is about, or where otherwise permitted by FIPPA legislation.

Security of Information - PHC is committed to maintaining the security of Personal Information and other sensitive information, including appropriate physical security of records and security safeguards for computer and network systems. Staff are expected to comply with PHC security requirements developed for use of such systems.

All Staff have the responsibility to protect against unauthorized access and disclosure of Personal Information. This responsibility includes ensuring that access or disclosure is only made to or by authorized individuals and reasonable measures are taken to prevent any unauthorized access, disclosure, loss or theft of information.

Compliance Monitoring, Auditing & Consequences - Access, use, disclosure and sharing of Personal Information will be monitored and all suspected breaches of the Information Privacy & Confidentiality Policy will be investigated by the Information Access and Privacy Office. Actions to be taken will be determined by Human Resources, Legal Services and/or other PHC stakeholders according to the nature of the breach and parties involved.

Breach of Policy – Staff are expected to report to the PHC Information Access & Privacy Office any breach of the Information Privacy & Confidentiality Policy, any concerns with or recommended improvements to information privacy and security procedures, and any information to help resolve problems. Staff may report real or suspected breaches without any fear of reprisal. Such reports will be covered by the PHC policy that protects "whistle blowers" (CPF1500 *Protection of Staff Who Report Financial Improprieties or Other Misconduct*).

If you have any questions, contact the PHC Information Privacy Office at: 604-806-8336 or privacy@providencehealth.bc.ca