Auditing Access to Clinical Information Systems

1. Introduction

Providence Health Care (PHC) is committed to ensuring that all personal information under its custody or control is collected, accessed, used, disclosed in a way that complies with the BC *Freedom of Information and Protection of Privacy Act* (FIPPA) and follows appropriate principles and best practices for information privacy, confidentiality and security.

Section 30 of FIPPA states that "a public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal". Auditing access to health records contained in or made accessible through Clinical Information Systems (CIS) is an important mechanism to comply with privacy legislation and PHC policies.

1.1. Purpose

The purpose of this policy is to:

- Communicate PHC audit processes and accountabilities to Staff and other users of Clinical Information Systems;
- Reduce unauthorized access to EHRs;
- Mandate appropriate audit controls and mechanisms to protect EHRs from inappropriate and unauthorized access; and
- Support a privacy-conscious environment within PHC.

1.2. Scope

This policy applies to all Staff and Clinical Information Systems that contain or provide access to personal information.

2. Policy

PHC will comply with the privacy and security requirements of FIPPA and apply best practices to implement Privacy Audit Programs and appropriate audit accountabilities for PHC.

2.1. Reactive Auditing Program

PHC shall maintain an incident-based auditing program for Staff, patients, residents and others to report potential unauthorized or inappropriate access to EHRs to the PHC Information Access & Privacy Office (IAPO). PHC will also respond to patient/resident/client requests for audits of their health record. The IAPO will investigate these reports and respond to potential privacy breaches in accordance with PHC Corporate Policy B-00-11-10120: Managing Privacy Breaches.

2.2. Proactive Auditing Program

PHC will maintain a proactive auditing program that:

a) Defines the scope of systems that will be subject to the proactive auditing program, including PHC core electronic patient care information systems;
b) Defines the processes and procedures for the administration of the proactive auditing program;
c) Defines the roles and responsibilities of PHC departments and Staff with respect to proactive auditing, and
d) Defines standardized fields for ongoing operation of the Privacy Audit Programs that apply to the CISs.

3. Responsibilities

3.1 Information Access and Privacy Office (IAPO)

a) Maintain and administrate this policy;
b) coordinate and conduct the initial investigation of potential and actual privacy breaches brought to its attention through the Privacy Audit Program;
c) assist Human Resources, Leaders, Managers, Department heads, and Physician Leaders, as required, to investigate privacy breaches by Staff;
d) support other Health Organization's privacy offices for investigations related to Lower Mainland consolidated services;
e) report breaches of privacy in accordance with PHC Managing Privacy Breaches policy; including to the Office of the Information Privacy Commissioner and members of the Senior Leadership Team, as appropriate;
f) notify or making recommendations to notify affected individuals as appropriate; and
g) provide education to staff with respect to the Privacy Audit Programs.

3.2 Human Resources/Medical Affairs

a) Provide employment information about staff to support investigations;
b) advise on appropriate disciplinary actions to be taken for staff who have been determined to have committed a privacy breach;
c) work with leaders/managers to ensure that disciplinary action for privacy breaches is carried out in accordance with Human Resource policies and procedures, and
d) report to IAPO whether disciplinary action was taken.

3.3 Leaders/Managers/Department Heads/Physician Leads

a) Ensure staff are aware of this policy and the Privacy Audit Programs;
b) advise the IAPO of any suspected unauthorized or inappropriate access to EHRs by others in accordance with this policy;
c) cooperate and participate in privacy breach investigations as requested;
d) determine, in consultation with the IAPO and Human Resources/Medical Affairs, whether access to EHRs by their staff are authorized and appropriate;
e) work with Human Resources/Medical Affairs to ensure that appropriate disciplinary actions are taken when staff have committed a privacy breach; and
f) undertake remedial and preventative follow-up action as recommended by the investigation.

3.4 Staff

a) Comply with applicable organizational privacy policies and terms of use/ policies applicable to CISs;
b) Report suspected unauthorized or inappropriate access to EHRs by others in accordance with this policy; and
c) Cooperate with investigations and collaborate with the IAPO on reasonable steps to prevent a recurrence.

3.5 Information Management/Information Technology Systems (IMITS)

a) Make information and technology resources available for conducting audits to support Privacy Audit Programs; and
b) work with the IAPO to establish standards for audit capabilities in Clinical Information Systems containing or providing access to Personal Information.

4. Compliance

Failure to comply with this policy may result in disciplinary action including, but not limited to, the termination of employment, loss of privileges as a student or volunteer role, loss of privileges in accordance with the Medical Staff Bylaws and Medical Staff Rules, prosecution and restitution for damages.

5. Supporting Documents

5.1 Related Policies

B-00-11-10108 Information Privacy and Confidentiality
B-00-11-10120 Managing Privacy Breaches
B-00-11-10119 Safe Reporting

6. Definitions

"CIS" (Clinical Information System) means any electronic information system containing recorded information about the health of an identifiable individual.

"EHR" (Electronic Health Record) means any recorded information about the health of an identifiable individual contained in or made accessible through electronic information systems.

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

"IAPO" means the Information Access and Privacy Office

"Patients & Residents" mean all individuals, including Assisted Living Tenants and Clients, who receive services from PHC.

"Personal Information" means recorded information about an identifiable individual other than contact information, such as a person's title, business telephone number, business address, email or fax number.

"Privacy Audit Programs" means activities and programs conducted by PHC to audit access to EHRs.

"Privacy Breach" occurs when there is an intentional or inadvertent unauthorized collection, use, disclosure, or disposal of personal information. Such activity is "unauthorized" if it occurs in contravention of the BC *Freedom of Information and Protection of Privacy Act (FIPPA)* and PHC's Confidentiality Policy (CPF0300). For the purpose of this policy, privacy breaches are managed the same whether suspected or confirmed.

"Reasonable Security" 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.

"Staff" means all employees (including management and leadership), medical staff members (including physicians, midwives, dentists) and nurse practitioners, residents, fellows and trainees, health care professionals, students, volunteers, contractors, researchers and other service providers engaged by PHC.

7. References

BC *Freedom of Information and Protection of Privacy Act*

OIPC Guidelines of Audits of Automated Personal Information Systems

Effective Date:	01-MAR-2009		
First Released:	01-MAR-2009		
Last Revised:	01-OCT-2022		
Last Reviewed:	01-OCT-2022		
Approved By:	PHC		
	Shaf Hussain		
Owners:	PHC		
	Information Access & Privacy Office		

Revision History: *(optional)*	**Version**	**Date**	**Description/ Key Changes**	**Revised By**
		01/OCT/2022	No material changes	Janet Scott