Approval Date	*July 8, 2021*
Revision Date	*May 2013, January 27, 2021*
Approved by	*Andree Robichaud, CEO*
Approver Signature	
Scheduled Review Date	*July 2023*
Cross- Reference	*4-h-20 Auditing Access to Clinical Information Systems*

PURPOSE

The purpose of this policy is to outline the authority and accountability for monitoring and auditing access to personal health information contained within clinical information systems of Central Health.

SCOPE

This policy applies to all Central Health employees and affiliated individuals who have access to clinical information systems of Central Health.

DEFINITIONS

Affiliated Individual	Individuals who are not employed by Central Health but perform specific tasks at or for the organization including, but not limited to, trustees, students, volunteers, pastoral care, researchers, contractors, vendors and individuals working at the organization but funded through an external source.
Audit	A manual or systemic assessment of end-user access to a clinical information system.
Appropriateness of Access	For this policy appropriateness of access is based on job specific requirements, access, disclosure or use of clinical or demographic information for the purpose of health care

	services, payment or services provided to the individual.
Circle of Care	The persons participating in and activities related to the provision of health care to the individual who is the subject of the personal health information and includes necessarily incidental activities such as laboratory work and professional consultation.
Client	A person who avails of the services of an authority, and includes a client, patient and/or resident.
Clinical Information Systems	For the purpose of this policy, refers to Meditech.
Personal Health Information	Identifying information in oral or recorded form about an individual that relates to: • Information concerning the physical or mental health of the individual, including information respecting the individual's health care status and history and the health history of the individual's family; • The provision of health care to the individual, including information respecting the person providing the health care; • The donation by an individual of a body part or any • bodily substance, including information derived from the testing or examination of a body part or bodily substance; • Registration information; • Information about the individual that is collected in the course of, and is incidental to the provision of a health care program or service or payment for a health care program or service; • Payments or eligibility for a health care program or service in respect of the individual, including eligibility for coverage under an insurance or payment arrangement with respect to health care; • An individual's entitlement to benefits under or participation in a health care program or service; • A drug as defined in the Pharmacy Act, a health care aid,

	device, product, equipment or other item provided to an individual under a prescription or other authorization issued by a health care professional; or • The identity of a person's representative as defined in Section 7 of the *Personal Health Information Act*.
Proactive Audit	For the purpose of this policy, an audit where access to personal health information may be performed with the use of auditing tools such as algorithms. For example, the same name exception, algorithm compares and analyzes the last name of the client against the same last name of an end user.
Privacy	The right of an individual, within limits, to determine when, how and to what extent personal information is collected, used and disclosed about themselves.
Privacy Breach	A privacy breach occurs when there is unauthorized and/or inappropriate access, collection, use, disclosure or disposal of personal information. Such activity is "unauthorized" if it occurs in contravention of ATIPPA or PHIA. The most common privacy breaches occur when personal information of clients, employees or corporate is stolen, lost or mistakenly disclosed. For example, a privacy breach occurs when a computer containing personal information is stolen or personal information is mistakenly emailed or faxed to the wrong person.
Reactive Audit	For the purpose of this policy, an audit conducted at the request of a client, their authorized representative or any manager/director/senior leader with a legitimate privacy concern that is authorized as per this policy.

POLICY STATEMENT(S)

Central Health has a legal and ethical obligation to protect personal health information (hereinafter referred to as Information) in its custody or control from unauthorized access, collection, use and/or disclosure in any format, including information contained in clinical information systems of Central Health.

Electronic auditing of access to clinical information systems is necessary to:

- determine compliance with and measure the effectiveness of Central Health's information security and privacy policies, processes and standards;
- ensure accountability for legislative requirements;
- ensure appropriate measures are in place for controlling access to information;
- monitor an individual's access to ensure compliance with rights of access to personal health information; and
- motivate all employees and affiliated individuals to honor privacy standards and policies.

Employees and other affiliated individuals (hereinafter referred to as End-users) with access to clinical information systems must be supported in having appropriate access to information that is relevant to performing their assigned duties, while being held accountable in the event they are found to be utilizing any form of information in an inappropriate manner.

Managers/directors/senior leaders/medical services representatives, in collaboration with the Information Management and Technology Department (IM&T), are responsible to ensure that end-users who require access to electronic clinical information systems have appropriate access in alignment with their job functions.

The Information, Privacy and Regulatory Oversight Department is responsible for monitoring compliance with policies and standards governing privacy and appropriate access to information by performing access audits on clinical information systems to ensure effective technical controls are in place to protect the confidentiality and privacy of the information.

When accessing clinical information systems to view information, End-users must have a provider/service relationship with the client or require access for other assigned duties of Central Health. Review or access of clinical information systems outside of one's authorized duties is not permitted. Examples include,

but are not limited to **unauthorized** access to:

- one's own personal health information;
- information of any of the End-user's direct/indirect family members;
- information relating to End-user's neighbours, friends, co-workers, acquaintances or public figures; or
- information of any other individual where the end-user is not included in the "circle of care" or does not require access for other assigned duties of their role.

Central Health's electronic auditing of clinical information systems is described as:

- Proactive (regular audits, random selection)
- Reactive (end-user/client-specific audits)
  - client request
  - internal request (manager, director, senior leader, medical services representative)
- Targeted audits completed at the discretion of Central Health's Chief Executive Officer or designate and/or Privacy Manager in response to circumstances such as:
  - End-users who have been found to be accessing clinical information systems outside of their authorized duties, thereby prompting a more detailed audit investigation;
  - End-users who have already received disciplinary action as a result of a privacy incident;
  - clients and/or situations that have resulted in media coverage;
  - clients with a highly sensitive diagnosis; and
  - clients who are considered "high profile".

Access audits can be conducted at the request of a client/authorized representative or manager/director/senior leader/medical services representative of a department/program. Completion of FRM-PHI002 (Systems Audit Request Form) will fulfill this requirement.

Where an access audit request is received from a Central Health employee or physician that is not in relation to their own information, the request must

be directed to the central health privacy representative. An audit request received from a Central Health employee or physician in relation to their own information is processed as a client request.

Access audits can be conducted on the basis of a specific client record accessed or on a specific end-user's access; Requests are subject to system capacity depending on the type of request received.

Where Central Health receives a request for an access audit from a client or their authorized representative, the access audit will be completed for the time period requested up to a maximum of a two (2) year period prior to the date of receipt of request.

Where a manager/director/senior leader/medical services representative of Central Health requests an access audit and the outcome of the audit identifies a privacy incident/breach, a more extensive access audit may be completed up to an additional two (2) year period prior to the date of potential privacy incident/breach.

Where an access audit reveals irregularities or anomalies, confirmed malicious intent or reckless negligence, investigations will be conducted by the department/program manager/director/senior leader/medical services representative in collaboration with the privacy representative.

Determining appropriateness of access may be supported by, but is not exclusive to, evidence that the end-user had documented in the client's record, provided service to the client, provided diagnostic testing; or for administrative functions such as financial and supportive services, where access is required to perform End-user assigned duties.

When there is a potential privacy incident/breach involving unauthorized access, collection, use or disclosure of information, it is the manager/director/senior leader/medical services representative and/or human resources designates responsibility to review the findings with the End-user suspected of the potential privacy incident/breach, and to confirm whether there was a failure to comply with Central Health's privacy and

security policies.

Any deliberate misuse, unauthorized access or disclosure or failure to safeguard information that has been confirmed will be subject to disciplinary action as per Central Health's People and Culture policies, Medical Services Bylaws or collective agreements and may be reportable to the End- user's regulatory body, where applicable.

Where unauthorized access involves an End-user that is not an employee or an affiliated health care professional of Central Health, an investigation that reveals failure to safeguard and/or unauthorized access, collection, use or disclosure of information will be subject to review of contract or service provision.

When there has been confirmation of a privacy breach, the discipline may include additional mandatory privacy awareness training, suspension/termination of employment or engagement of contract services, and/or loss of hospital privileges as applicable. Discipline will be applied in relation to the sensitivity of information accessed, used or disclosed and the nature and severity of the privacy breach.

Where resources permit, End-users' names that appear on an access audit and their access has been deemed as appropriate, the End-user will be notified in writing to that effect by the privacy representative, or as otherwise delegated.

Any recommendations for improvement of confidentiality and privacy practices will be evaluated by Central Health's Privacy Manager, in collaboration with the director of the department/program/senior leader or VP of Medical Services.

Central Health recognizes the necessity of conducting access audit requests in a timely manner. Requests will be processed in an approved manner on a case-by-case basis; however, there must be compliance with the legislative timeframe to complete a request for disclosure of access audit results within sixty (60) days of receipt of the request.

When a client or authorized representative requests a copy of an access audit, a copy of the access audit will be provided to the requestor; however, a discussion outlining the access processes and requirements will be provided to the requestor prior to disclosure of the access audit.

Where an access audit confirms a privacy breach, the manager/director/senior leader/medical services representative will enter an occurrence as per Central Health's occurrence reporting system and refer to Central Health's Privacy Breach Policy.

Where Central Health receives a privacy complaint concerning a suspected inappropriate access, the complaint must be entered as per Central Health's occurrence reporting process.

Access audits and outcomes will be treated as confidential by the same access and security standards and policies as other confidential information.

A summary access audit activity report will be provided to the Director of Information, Privacy and Regulatory Oversight on a monthly basis for statistical purposes and compliance reporting to the senior leader.

PROCEDURE

Electronic access auditing is conducted in the following formats:

Automated Audit Process

Access audit protocols are conducted by the privacy representative or delegate on a regular basis from automated standard exception reports such as same last name match, same street name match, guarantor/subscriber/user name match, provider/user location activity match, etc., as per Central Health's auditing access schedule.

Statistics are retained indicating the auditing activities performed within Central Health (i.e.: number of audits per system, number of end-users

identified on each report, algorithm type, pattern of usage, anomalies identified, actions and recommendations, etc.).

Requested Access Audit Process

The requestor makes the request through the Information, Privacy and Regulatory Oversight Department privacy representative by completing FRM-PHI002 (Systems Audit Request).

The privacy representative:

a. ensures the Systems Audit Request Form is date stamped and logged as received;
b. confirms the requestor has the authority to request access audit (i.e., authorized representative, authorized manager/director);
c. contacts requestor if clarification of access audit request is required;
d. forwards notification letter to the requestor confirming receipt of access audit request;
e. initiates access audit;
f. follows investigation process outlined below;
g. where **no** identified privacy breach occurs, provides verbal notification to the requestor;
h. forwards a standard letter in follow-up of conversation to the requestor; and
i. ensures access audit request and follow-up letter is retained on client's record where applicable.

Investigation of Access Audit

The privacy representative:

a. conducts and reviews results of the access audit to determine appropriateness of access as per defined audit cues;
b. where an access audit identifies a potential incident/breach or where the relationship of the end-user cannot be determined, flags access audit;

c. completes **Part A of FRM-PHI010 (Access Audit Follow-up Report),** forwards form and provides results of access audit to the manager/director/senior leader/medical services representative for further review and follow-up;
d. provides timeframe to the manager/director/senior leader/medical services representative for completion of access audit review;
e. where required, in collaboration with the manager/director/senior leader/medical services representative, assists in the investigation of the access audit; and
f. retains a copy of access audit until the Access Audit Follow-up Report is returned by the manager/director/senior leader/medical services representative.

Where a privacy breach IS NOT identified:

a. the manager/director/senior leader/medical services representative completes the Part B of FRM-PHI010 (Access Audit Follow-up Report) and forwards it to the privacy representative;
b. the privacy representative or designate tracks the outcome of the Access Audit Follow-up Report for statistical purposes.

When a privacy breach is identified:

The manager/director/senior leader/medical services representative:

a. conducts an investigation in consultation with the privacy representative;
b. enters an occurrence report as per Central Health's occurrence reporting system and refers to the Privacy Breach Policy;
c. consults with the human resources representative or, where

applicable, the VP of Medical Services for guidance in addressing inappropriate access;

d. upon completion of investigation, completes Part B of FRM-PHI010 (Access Audit Follow-up Report) and forwards to the privacy representative.
e. The completed Access Audit Follow-up Report is retained on the personnel file of the employees/affiliated individual within People & Culture [Formally Human Resources].

Where an individual(s) is affected by a privacy breach, the notification process will be determined by Central Health's Privacy Manager, senior leader and other stakeholders as per the Privacy Breach policy.

REFERENCES

Eastern Regional Health Authority (2010), Auditing of Access to Electronic Health Records, (IMT-050).

Information and Privacy Commissioner of British Columbia, OPIC Guideline 01-01, October 10, 2001. p. 1-8.

NHS Business Partner, Information Governance Toolkit, R9-206, v9.0. p.1-8.

Personal Health Information Act, Statutes of Newfoundland and Labrador (2008, c. P-7.01). Retrieved from the House of Assembly Newfoundland and Labrador website: http://assembly.nl.ca/legislation/sr/statutes/p07-01.htm

Saint Louis University, INFOSEC 1.5 Internal and External Audit, Version 1.0, May 18, 2010. p. 1-5.