CATEGORY:	**ORGANIZATIONAL: INFORMATION MANAGEMENT**
SUB-CATEGORY:	**INFORMATION MANAGEMENT**
GROUP:	
DISTRIBUTION:	**ALL STAFF/PHYSICIANS**
TITLE:	**AUDITING ACCESS TO CLINICAL INFORMATION SYSTEMS**

PURPOSE

To outline the authority and accountability for monitoring and auditing access to personal health information contained in Western Health's clinical information systems.

POLICY

Western Health has a legal and ethical responsibility to ensure that personal health information in its custody and control is protected against theft, loss and unauthorized access, use or disclosure.

The organization also has an obligation to ensure that users are supported in having appropriate access to information that is relevant to performing their assigned duties on a "need to know" basis.

Designated Information Management employees are responsible for monitoring and auditing access to personal health information contained in Western Health's clinical information systems, and must conduct investigations when audits reveal irregularities, repeated lapses, malicious intent or reckless negligence.

In collaboration with designated Information Management employees, immediate managers or designates are responsible to ensure that employees under their supervision as well as other affiliated individuals (hereinafter both referred to as end users) are granted appropriate access to clinical information systems in keeping with their assigned duties.

When accessing clinical information systems to view personal health information, end users must have a provider/service relationship with the client, or require access as part of their assigned duties within Western Health. End users **must not** access personal

information/personal health information (hereinafter referred to as information) outside their assigned duties.

Examples include any **unauthorized** access to:

- One's own information;
- The information of any of the end user's family members;
- The information relating to the end user's neighbours, friends, co-workers, acquaintances or public figures;
- The information of any other individual where the end user is not included in the "circle of care" (see definition), or does not require access for other assigned duties within Western Health.

To obtain access to their own health record, all clients/patients/residents (including employees/physicians) must contact the Health Records Department at the site/facility where their record is located, or contact their service provider.

Any deliberate misuse, inappropriate disclosure, or failure to safeguard information that has been confirmed will be subject to disciplinary action as per applicable Western Health policy, Medical Services Bylaws or respective collective agreements and may be reportable to the end user's regulatory body.

Where unauthorized access involves an end user who is not an employee or health care provider of Western Health, an investigation revealing a failure to safeguard and/or unauthorized access to information will be subject to review of the contract or service provision.

Audit requests and results must be treated as confidential by the same access and security standards and policies as other confidential information.

Requests for audits of non-clinical applications such as Web Services, Outlook and other databases must be directed to the Regional Director Information Management.

Auditing of access to electronic clinical information systems may take two forms: proactive and reactive.

1. Proactive Auditing

The Regional Privacy Analyst or designate must regularly generate proactive audits in collaboration with immediate managers or designates in other programs/departments/services, as appropriate.

The Regional Privacy Analyst or designate and/or immediate manager must:

a) Generate and review audits to determine appropriate access as per defined audit cues, and in consideration of the end user's assigned duties;
b) Where audits indicate a potential privacy occurrence, complete Part A of the *Clinical Information Systems Audit Follow Up* form (*Form #12-2450)* and forward it to the employee's immediate manager or designate;
c) Through review of Part A of the *Clinical Information Systems Audit Follow Up* form, (Form #12-2450) determine whether a privacy breach has occurred.

Where upon review of the audit information a privacy breach IS NOT identified:

a) The immediate manager or designate must complete Part B of the *Clinical Information Systems Audit Follow Up* form (Form #12-2450) and forward it to the Regional Privacy Analyst or designate.

Where upon review of the audit information a privacy breach IS identified:

a) The immediate manager or designate must:
   i) Ensure that an Occurrence Report is completed in keeping with Western Health's *Occurrence Reporting* policy (6-02-15);
   ii) Conduct an investigation in consultation with the Regional Manager Information Access and Privacy / Privacy Analyst and other departments, as required;
   iii) Complete Part B of the *Clinical Information Systems Audit Follow Up* form (Form #12-2450) and forward it to the Regional Privacy Analyst or designate.

b) Work with the Regional Manager Information Access and Privacy / Privacy Analyst and other Managers/Directors/Vice Presidents, as required, to determine the most appropriate disclosure process in keeping with Western Health's *Disclosure of Occurrences* (6-02-16) and *Privacy Breach Management* (9-03-10) policies.

2. Reactive Auditing

Clients/patients/residents, their authorized representatives or any other individual expressing a privacy concern may request an audit of their records. At the request of the Chief Executive Office, Regional Director Information Management or their designates, triggered audits may also be conducted in response to circumstances as outlined in this policy (see definition of triggered audit.)

a) Audit requests must be made through the Regional Privacy Analyst or designate by completing a *Clinical Information System Audit Request* form (Form #12-2455). Employee requests for an audit of the record of a client/patient/resident record must be first discussed with the immediate manager or designate. However, this is not required when the request is for an audit of the employee's own personal health information or that of a family member for whom they are an authorized representative. (In such cases, the employee must complete the Client/Patient/Resident portion of the form only.)

b) Audits may be conducted based on access to the record of a particular client/patient/resident or specific to the access by an identified end user, within system capacity.

c) In exceptional circumstances, where a requestor (normally a client/patient/resident) is unable to complete a *Clinical Information Systems Audit Request* form (Form #12-2455), the person who receives the request must document it on the form.

d) Audits will be conducted for a maximum of the previous two years activity from the date of the request. A more extensive audit may be performed at the discretion of the Regional Manager Information Access and Privacy or designate. All audit requests are subject to limitations based on the availability of information.

e) Where a privacy breach is suspected, the Regional Manager Information Access and Privacy or designate must complete a *Clinical Information Systems Audit Follow Up* form (Form #12-2450) and forward to the employee's immediate manager or designate for completion.

Where upon review of the audit information a privacy breach IS NOT identified:

a) The immediate manager or designate must complete Part B of the *Clinical Information Systems Audit Follow Up* form (Form #12-2450) and return it to the Regional Manager Information Access and Privacy or designate.

b) The Regional Manager Information Access and Privacy or designate must provide notification to the requestor outlining the audit results.

Where upon review of the audit information a privacy breach IS identified:

a) The immediate manager or designate must:
   i) Ensure that an Occurrence Report is completed in keeping with Western Health's Occurrence Reporting policy (6-02-15);
   ii) Conduct an investigation in consultation with the Regional Manager Information Access and Privacy / Privacy Analyst and other departments, as required;
   iii) Complete Part B of the *Clinical Information Systems Audit Follow Up* form (Form #12-2450) and forward it to the Regional Privacy Analyst or designate.

b) Work with the Regional Manager Information Access and Privacy / Privacy Analyst and other Managers/Directors/Vice Presidents, as required, to determine the most appropriate disclosure process in keeping with Western Health's *Disclosure of Occurrences* (6-02-16) and *Privacy Breach Management* (9-03-10) policies.

DEFINITIONS

Affiliated individual: For the purpose of this policy, individuals who are not employed by Western Health, but perform specific tasks at or for the organization, including, but not limited to trustees, students, volunteers, researchers, contractors, vendors, and individuals working at Western Health, but funded through an external source.

Audit / auditing: Refers to a manual or systematic assessment of end user access to a clinical information system. Auditing of clinical information systems may be:

a) Proactive: An audit where access to personal health information may be performed with the use of tools, such as algorithms. For example, the "same name" algorithm compares the last names of end users against the same last names of clients of Western Health. In addition, random end user audits may also be conducted for a specific time frame, at the discretion of the Regional Manager Information Access and Privacy or designate and/or the Information Management / Technology Department.
b) Reactive: An audit conducted at the request of a client or his/her authorized representative, or any other person with a legitimate privacy concern that is authorized as per this policy.

Triggered audits may also be completed at the request of the Chief Executive Officer or designate and/or the Regional Manager, Information Access and Privacy or designate in response to circumstances such as:

- End users who have been found to be accessing clinical information systems outside his/her authorized duties and 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;
- Clients who are considered "high profile."

Circle of care: Describes the health care professionals, providers and persons/entities who are participating in activities related to the provision of care to a client who is the subject of the personal health information and therefore, form the client's/patient's/resident's health care team.

Individuals/entities that may be included in a client's/patient's/resident's circle of care include:

- health care professionals, such as doctors, nurses, as well as those who perform necessarily incidental functions, such as laboratory and diagnostic services, as well as a range of professional consultation services;
- a health care provider, meaning a person or entity other than a health care professional, who is directly or indirectly paid, in whole or in part, by MCP, another insurer or person, to provide health care services to an individual;
- a person who operates:
  - a health care facility;
  - a licensed pharmacy, as defined in the Pharmacy Act;
  - an ambulance service; or
  - a centre, program or service for community health or mental health, with the primary purpose being the provision of health care by a health care professional or health care provider;
- any person or entity that is providing health care to the client/patient/resident, such as family members, home care workers, etc.

Confidential business information: Information with respect to Western Health's business that is not publicly disclosed by the organization. Employees / affiliates may come in contact with such information that is not generally known to the public as they perform their duties. Examples include:

a) Legal matters involving the organization that are not public knowledge,
b) Financial information that is not available in Western Health's annual report,
c) Contractual agreements with vendors, consultants, contractors, and third parties (The confidentiality of this information may be written into the contract, e.g. non-disclosure of the cost of the service),
d) Information about intellectual property such as development of new technology and treatments or unpublished reports,
e) Information pertaining to Western Health's information technology access and security systems such as:
f) Information that could lead to inappropriate access to internal and external computer resources,
g) Information that is regarded as confidential between the vendor and Western Health related to negotiated product discounts,
h) Products that are part of Western Health's security infrastructure or the names of vendors of hardware / software solutions that may be vulnerable to external access attacks.

Personal information: Information of an identifiable individual, but does not include the name, title, business address / telephone number of a staff member of an organization.

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;
- 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;
- 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 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*.

Privacy: The right of individuals to control the collection, use and disclosure of information about themselves.

Privacy breach: Occurs when there is unauthorized and/or inappropriate access, collection, use, disclosure or disposal of personal information / personal health information. Such activity is "unauthorized" if it occurs in contravention of the *Access to Information and Protection of Privacy Act* (ATIPPA) or the *Personal Health Information Act* (PHIA.) The most common privacy breaches occur when personal information / personal health information of clients/patients/residents, employees or confidential business information of Western Health is stolen, lost or mistakenly disclosed. For example, a privacy breach occurs when a computer containing personal information / personal health information is stolen or personal information / personal health information is emailed or faxed to the wrong person in error.

LEGISLATIVE CONTEXT

Access to Information and Protection of Privacy Act (2004). Available at: http://www.assembly.nl.ca/legislation/sr/statutes/a01-1.htm

Personal Health Information Act (2008). Available at: http://www.assembly.nl.ca/legislation/sr/statutes/p07-01.htm

REFERENCES

Central Health (2012). *Auditing Access to Electronic Personal Health Information*

Labrador-Grenfell Health (2012). *Auditing Access to Clinical Information Systems*

Newfoundland and Labrador Health and Community Services (May 1, 2013). *Regional Health Authority Meditech Privacy Auditing, Reporting, and Public Notification Policy*

KEYWORDS

Audits, auditing health records, client records, audit, auditing, access, access to information, privacy breach, privacy, personal health information, health information, protection of privacy, confidential information, confidentiality, circle of care,

FORMS

Clinical Information System Audit Request (Form #12-2455)

Clinical Information Systems Audit Follow Up (Form #12-2450)

TO BE COMPLETED BY QUALITY MANAGEMENT & RESEARCH STAFF ONLY

Approved By: Chief Executive Officer	Maintained By: Regional Manager Information Access & Privacy
Effective Date: 04/July/2007	❒ Reviewed: ☑ Revised: 13/March/2015
Review Date: 13/March/2018	☑ Replaces: (WH) 10-01-20 Electronic Health Record User Access Review ❒ New