Labrador-Grenfell Health

SUBJECT: **AUDITING OF ACCESS TO CLINICAL INFORMATION SYSTEMS**
APPROVED BY: Chief Executive Officer _____
EFFECTIVE DATE: 2012 11
REVIEW/REVISED DATE:

Purpose:

To outline the authority and accountability for monitoring and auditing access to personal health information contained within clinical information systems of Labrador-Grenfell Health.

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

- Determine compliance with and measure the effectiveness of Labrador-Grenfell Health's information security and privacy policies and standards;
- Determine compliance with and outline accountability for legislative requirements;
- Outline appropriate measures for controlling access to information;
- Monitor systems to determine appropriateness of access to clinical information;
- Motivate all employees and other affiliated individuals (herein referred to as "end users") to adhere to privacy standards and policies.

Policy/Standard:

Labrador-Grenfell Health has a legal and ethical responsibility to protect personal health information from unauthorized access, collection, use and/or disclosure in any format, including information that is contained in clinical information systems. End users 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 personal health information in an inappropriate manner. Therefore, access to clinical information systems must be monitored in order to protect clients' privacy rights, while also determining organizational compliance with mandatory privacy laws and regulations.

When accessing clinical information systems to view personal health information, end users must have a provider/service relationship with the client, or require access for other assigned duties of the Health Authority. Review or access of clinical information systems outside of one's authorized duties is not permitted. Examples include, but are not limited to, any **unauthorized** access to:

- one's own personal health information;
- personal health information for any of the end user's direct/indirect family members;
- personal health information relating to the end-user's neighbors, friends, co-workers, acquaintances or public figures;
- personal health information for any other individual where the end user is not included in the "circle of care" (see definition below), or does not require access for other assigned duties of the Health Authority.

Investigations will be conducted when audits reveal irregularities, anomalies, repeated lapses, malicious intent or reckless negligence.

Any deliberate misuse, inappropriate release or failure to safeguard information that has been confirmed will be subject to disciplinary action as per Labrador-Grenfell Human Resources policy, Medical Services Bylaws or respective collective agreements and may be reportable to the end user's professional regulatory body (where applicable).

Where unauthorized access involves an end user that is not an employee or health care provider of Labrador-Grenfell Health, an investigation that reveals failure to safeguard and/or unauthorized access to information will be subject to review of the contract or service provision.

Audit requests and results will be treated as confidential by the same access and security standards and policies as other confidential information and will be retained in accordance with Labrador-Grenfell practices.

Definitions:

"Auditing" is a manual or systematic assessment of end user access to a clinical information system. Auditing of clinical information systems can be:

- ***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 name of end users against the same last names of clients of Labrador-Grenfell Health. In addition, random end user audits may also be conducted for specific timeframes, at the discretion of the Regional Privacy Office or designate.

- ***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 discretion of the Chief Executive Officer or designate and/or the Regional Privacy Office in response to circumstances such as:

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

"Circle of Care" describes the health care professionals, providers and persons/entities that 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 health care team.

Individuals/entities that may be included in a client'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, such as family members, home care workers, etc.

<u>Materials Required</u>:

- Request for Audit of Access to Electronic Health Information Form P&A-9-035-1
- Access Audit of Electronic Health Information: Follow-Up Report Form P&A-9-035-2

Related Policies:

- Privacy and Confidentiality P&A-9-010
- Oath/Affirmation of Confidentiality P&A-9-020
- Security of Confidential Information P&A-9-030

Procedure:

Electronic access auditing may take two forms:

1. Proactive Auditing:
Proactive audits will be generated regularly by the Regional Privacy Officer or designate and reviewed in conjunction with other departments and managers/supervisors, as appropriate.

Depending on the report type, the Regional Privacy Officer or manager/supervisor will:
- Review the audit to determine appropriate access as per defined audit cues, or in consideration of the end user's authorized duties.
- Flag audits that indicate a potential privacy occurrence using *Part A* of the *Access Audit of Electronic Health Information Follow-Up Report* form (P&A-9-035-2).

Where a privacy breach IS NOT identified:
- The manager/supervisor will complete Part B of the Access *Audit of Electronic Health Information Follow-up Report* form (P&A-9-035-2) and forward to the Regional Privacy Office.

Where a privacy breach IS identified:
- The manager/supervisor will:
  - Contact the Regional Privacy Officer immediately;
  - Enter an occurrence report as per Labrador-Grenfell Health's electronic occurrence reporting system (Clinical Safety Reporting System, or CSRS);
  - Conduct investigation, in consultation with the Regional Privacy Office and other departments, as required;
  - Complete *Part B* of the *Access Audit of Electronic Health Information Follow-up Report* and forward to the Regional Privacy Office.

- The most appropriate disclosure process will be determined in consultation with the Regional Privacy Office, the Patient Safety and Quality and Communication departments and senior leaders, as required.

2. Reactive (Requested) Auditing:

Requests for auditing will be 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 discretion of the Chief Executive Officer or designate and/or the Regional Privacy Office in response to circumstances outlined.

- Audit requests will be made through the Regional Privacy Office via the completion of a *Request for Audit of Access to Electronic Health Information* form (P&A-9-035-1).
- Employee requests for auditing must be first discussed and approved with their immediate manager/supervisor, but is not required when the request is specific to the employee's own personal health information or that of a family member or another individual for whom they are an authorized representative.
- Audits may be conducted on the basis of a specific client record accessed or on a specific end-user's access, within system capacity.
- Where in exceptional circumstances a requestor is unable to complete this form, a verbal request will be accepted and documented on this form accordingly.
- A request for an access audit will be completed for a maximum of a two (2) year period back from the date the request was received. In exceptional circumstances, a more extensive audit may be performed. All audit requests are subject to limitations based on the availability of information.
- Where a privacy breach is suspected, the Regional Privacy Office will complete *Part A* of the *Access Audit of Electronic Health Information Follow-up Report* (P&A-9-035-2) and forward to the department/program manager/supervisor for further review. In cases where further details are required, the privacy manager/designate will also attach a copy of the auditing results to this form.

Where a privacy breach <u>IS NOT</u> identified:

- The manager/supervisor will complete Part B the Access *Audit of Electronic Health Information Follow-up Report* form and return to the Regional Privacy Office as soon as possible.
- The Regional Privacy Office will forward a standard notification letter to the requestor outlining audit results.

Where a privacy breach IS identified:

- The manager/supervisor will:
  - Contact the Regional Privacy Office immediately;
  - Enter an occurrence report as per Labrador-Grenfell Health's electronic occurrence reporting system (CSRS);
  - Conduct investigation, in consultation with the Regional Privacy Office and other departments, as required;
  - Complete *Part B* of the *Access Audit of Electronic Health Information Follow-up Report* and forward to the Regional Privacy Office.
- The most appropriate disclosure process will be determined in consultation with the Regional Privacy Office, the Patient Safety and Quality and Communication departments and senior leaders, as required.

Other Considerations:

Audit requests will be processed without delay on a case-by-case basis. However, the legislative timeframe to complete a request for disclosure of information is 60 days upon receipt of request; this time limit may be extended for an additional 30 days in extenuating circumstances. Where an extension is required, written notice of the extension and reason thereof must be provided to the requestor.

A report on audit activity will be generated on a regular basis for compliance and statistical purposes.

References

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

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

Province of Newfoundland and Labrador (2008). *Personal Health Information Act, SNL 2008, c. P-7.01*.
Retrieved from: http://assembly.nl.ca/Legislation/sr/statutes/p07-01.htm