eHealth Ontario

Auditing and Monitoring Guide

Electronic Health Record

Version: 1.0

Ontario
eHealth Ontario

Copyright Notice

All rights reserved

Trademarks

Document Control

The electronic version of this document is recognized as the only valid version.

Revision History

VERSION NO.	DATE YYYY-MM-DD	SUMMARY OF CHANGE	CHANGED BY
1.0	2016-03-17	Final	Connecting Privacy Committee (CPC)
0.04	2016-03-10	Final Draft	CPC Logging and Auditing Working Group
0.03	2015-11-23	Third Draft	CPC Logging and Auditing Working Group
0.02	2015-11-09	Second Draft	CPC Logging and Auditing Working Group
0.01	2014-03-05	Initial Draft	CPC Logging and Auditing Working Group

1 Contents

1 Purpose/ Objective

The purpose of this guide is to provide guidance on auditing and monitoring privacy best practices. The guide aims to assist eHealth Ontario and Health Information Custodians (HICs) in deterring, detecting and preventing unauthorized access to personal health information (PHI) and to comply with relevant privacy requirements.

2 Scope

This guide applies to the auditing and monitoring of PHI that is viewed, handled or otherwise dealt with in relation to the Electronic Health Record. It is intended to be read with the *EHR Logging and Auditing Policy*. The EHR is comprised of the ConnectingOntario Solution and the Diagnostic Imaging Common Services Repository. The ConnectingOntario Solution and the Diagnostic Imaging Common Services Repository are classified as clinical repository and/or ancillary systems designed to store and make available specified electronic PHI from the electronic health information systems of HICs[1].

3 Guidelines

3.1 Types of Auditing and Monitoring

Provisioning access to users of electronic health information systems allows users quick and easy access to an increased number of health records. eHealth Ontario and HICs must take reasonable measures to deter, detect and prevent unauthorized access to records of PHI, including auditing and monitoring access to PHI.

eHealth Ontario and HICs may conduct auditing and monitoring once a suspected privacy breach has occurred; however eHealth Ontario and HICs must also address proactive and ongoing auditing and monitoring as described below.[2]

> Reactive Auditing and Monitoring:
> Reactive auditing and monitoring is conducted in response to a trigger such as an actual or suspected privacy breach or when an individual makes a complaint or a request to review access logs.
>
> Proactive Auditing and Monitoring:
> eHealth Ontario and HICs should conduct proactive auditing and monitoring over and above reactive audits to deter and detect unauthorized access to PHI. Proactive auditing and monitoring is conducted on a selection of all authorized users who access PHI and/or on a selection of individuals. Users and patients are selected for proactive auditing and monitoring either randomly or because there is considered to be an elevated risk of breach for the selected users or patients.
>
> Consent-related Auditing and Monitoring:
> eHealth Ontario and HICs should continually monitor all access to PHI to identify consent overrides, PHI accessed in the event of an override of a consent directive as well as every instance where a consent directive has been added, removed or modified. Remember that the *EHR Consent Management Policy* requires HICs to notify patients of consent overrides.

3.2 Frequency and Scope of Auditing and Monitoring

Organizations should take a risk based approach when deciding on scope and frequency of random audits to be able to maximize the impact of deterring, preventing and detecting unauthorized access with the investment required for auditing and monitoring.

[1] Variance in policy and procedure requirements between the ConnectingOntario Solution and the Diagnostic Imaging Common Services Repository is highlighted within the policy.

[2] Information and Privacy Commissioner of Ontario, *Detecting and Deterring Unauthorized Access to Personal Health Information* January 2015. Available online at https://www.ipc.on.ca/images/Resources/Detect_Deter.pdf.

3.2.1 Frequency

Ongoing monitoring should occur on a continuous frequency that allows organizations to manage privacy breaches in a reasonable time as well as to notify patients in a reasonable time that a consent directive override has occurred or a consent directive has been made, modified or removed[3].

While reactive auditing and monitoring occurs in response to a trigger event, the frequency of random auditing and proactive monitoring should be a risk based decision taking into account risk-related factors such as these:

- Size of the organization;
- Number of users;
- Frequency of access to PHI;
- Sensitivity of information;
- Access by third parties; and
- Previous privacy breaches and incidents.

It is recommended that organizations conduct proactive auditing and monitoring more frequently for users who have previously accessed PHI in an unauthorized manner or based on the risk level when considering the factors listed above.[4,5]

The frequency of auditing and monitoring should be done in-line with any commitments made in agreements. For example, section 4.5 of the *Electronic Health Record Access Services Schedule*[6] states the following:

> 4.5 The Privacy Officer or his/her delegate must generate or acquire, where available, from the Computer Application Provider an audit report on a subset of user access to the Computer Application and Client Systems on a quarterly basis.

3.2.2 Scope

Since it would be difficult to conduct audits of all access to PHI, eHealth Ontario and HICs should select which access logs to audit using a risk based approach, by considering, for example:

- Previous privacy breaches and incidents at the organization;
- Privacy breaches reported in the media (i.e. high profile client); and
- Consent directives.

3.3 Threat Use Cases for Monitoring

The list below consists of threat use cases that can be used when using a risk based approach to determining the frequency and scope of auditing and monitoring.[7] This list of use cases should be reviewed regularly (at least annually) and use cases should be reviewed when new Information and Privacy Commissioner of Ontario orders are issued, when new or reoccurring privacy breaches occur within your organization or when privacy breaches are reported in the media.

Threat use cases marked with an asterisk (*) are use cases that can be monitored by both eHealth Ontario conducting the audit and/or monitoring and the HIC for which the user is employed. Note that the eHealth Ontario must still monitor access logs, considering all of the use cases, for users (agents) working for the eHealth Ontario.

- A user accesses PHI outside of normal working hours.*
- A user logs in at two locations/computer terminals simultaneously or within a short period of time (near simultaneously).*
- A user is accessing PHI from an unusual location or facility (i.e. a physician who is staffed at a Toronto Hospital, is accessing records from a health care facility at Ottawa).

[3] Note: The *EHR Consent Management Policy* requires an organization to notify a patient that the patient's consent directive request has been implemented, immediately after confirming that the consent directive request has been implemented. The Policy also requires the Program Office to continuously audit and monitor access logs, and to immediately notify the relevant HICs when an override occurs. The Policy requires that HICs must notify the individual, whose records were accessed in the event of an override, at the first reasonable opportunity.

[4] Note: The *Alberta Electronic Health Records Regulation* requires the information manager of the Alberta EHR to conduct an audit each month of the information logs of the Alberta EHR.

[5] Monthly audits of all clinical information systems is recommended by the American Health Information Management Association (AHIMA) in 'Privacy and Security Audits of Electronic Health Information'

[6] eHealth Ontario. *Schedule – EHR Access Services*.

[7] AHIMA, Privacy and Security Audits of Electronic Health Information

- A user is accessing PHI associated with a department or treatment that is unrelated to his/her disciplines (i.e. a registration clerk accessing diagnostic imaging records).
- A user accesses his/her own PHI.*
- A user accesses PHI for a patient with the same last name as the user (indicating the user may be accessing PHI of a relative).*
- A user accesses PHI for a patient with the same address or street name as the user's address.
- A user is accessing PHI for a staff member who works at the same organization as the user.
- A user conducts a large number of patient searches for his/her job function.*
- A user accesses a large number of records over a short period of time for his/her job function.*
- A user accesses PHI after a long period of inactivity.*
- A user generates a lot of system errors, including for example, frequent login errors, or patient not found errors.*
- A user accesses PHI of a high profile patient or patient with a confidentiality flag.
- A user conducts a consent directive override to access a patient's PHI.*
- A user conducts a large number of consent directive overrides.*
- A user accesses sensitive PHI that is unrelated to his/her job duties, for example, psychiatric disorder, abortion records or records related to sexually transmitted diseases.
- A user accesses PHI for a patient that the user is not treating (the patient is not on the user's patient list).
- A user who is no longer employed at the organization (to verify that access has been rescinded).
- A user who has previously accessed PHI in an unauthorized manner, accesses PHI.

The individual reviewing the access logs should be familiar with the user's job functions and therefore be better able to evaluate potentially inappropriate access patterns. Privacy Officers reviewing audit logs should do so in consultation with user's managers and business subject matter experts. These individuals are able to add insight to interpret the threat use cases to the fullest potential. It is important to note that users who are part of a union may want to have a union representative available if they will be questioned about their user activity.

To assist in detecting suspected unauthorized access, eHealth Ontario or HIC may generate access reports indicating:

- All records of PHI that a specified user is accessing; and
- All users who accessed a specific patient.

3.4 Considerations for Automated Auditing and Monitoring Tools

Automated monitoring tools can assist in detecting suspected unauthorized activity by systematically reviewing access events and creating alerts whenever a certain trend or trigger is met (i.e. high number of access or a user accessed a patient with the same last name as the user). These tools can be particularly helpful when analyzing large quantities of data.

Trigger events can be pre-determined by a user based on one event (i.e. a user performs a consent override) or based on correlated events (i.e. a user accesses 5 PHI records within 10 minutes). Monitoring tools can also identify advanced triggers by correlating access events with other lists or logs (i.e. relating a user's patient list with a user's access events to generate an alert when a user accesses records of a patient that is not on the user's patient list). Once a trigger is met, an alert can be sent to a designated individual to investigate.

Technology solutions can also offer eHealth Ontario and HICs a quick and easy way to view access patterns, trends or averages over time. Users can view information through various means, including for example, graphs, dashboards and/or reports. Reports can be customized, filtered and/or sorted, for example, by facility, user, patient and/or date.

eHealth Ontario and HICs should balance the advantages of monitoring tools with the following considerations[8]:

- Cost to purchase and install the tool;
- Time and cost for training users;
- Time and/or costs for modifying threat use case, reports or other customizable options;
- Licensing and support fees; and
- Time for investigating alerts.

eHealth Ontario and HICs may consider procuring a managed service provider who owns and operates the monitoring tool on behalf of the organization. In this case, the organization would avoid the cost of purchasing and installing the system and the managed service provider would provide support to customize and program the application.

[8] AHIMA, Privacy and Security Audits of Electronic Health Information

3.5 Roles and Responsibilities

Access to logs should be restricted to only appropriately authorized users. An inventory of all access logs (or types of access reports that can be generated) as well as a description of each access log, the purpose for each access log, and the authorized user or recipient of each access log should be recorded to assist in ensuring access logs are only accessed and used for authorized purposes. To track compliance and ensure access logs are used only for authorized purposes, an inventory of all access logs generated or reviewed should be maintained, as well as any individual who used the access logs and the date of access.

It is beneficial if individuals who are most familiar with job responsibilities conduct an audit of their staff's access as they can best interpret findings and identify questionable circumstances that require additional investigation. In addition, the individual who is conducting the audit should have their accesses to PHI audited by another individual.

In addition to setting roles for individuals conducting auditing and monitoring, responsibilities with service providers who are hosting, providing technology to audit and/or monitor should be well documented in agreements and communicated to all relevant parties. Agreements should clarify who is responsible for creation, maintenance, and archiving of audit events. Considerations should be given to how long access logs will be retained, how long it will take to generate and make access reports available and how to change or update audit log criteria (i.e. types of access reports that can be generated as well as type of information included in the logs).

3.6 Awareness of Auditing and Monitoring Practices

Communicating auditing and monitoring practices can act as a strong deterrent to unauthorized access. Organizations should ensure visibility of auditing and monitoring practices by:

- Setting system reminders or warnings that indicate to a user that all access is audited and associated with the user name;
- Including appropriate auditing and monitoring terms in policies and end-user agreements;
- Including a description of logging, auditing and monitoring practices in training and/or awareness materials, including, for example, posting auditing and monitoring practices on your organizations website;
- Communicating that additional auditing practices may be introduced at any time, without prior notice:
- Notifying users who are the subject of any audit, including random audits, that logs related to his/her access to PHI is under review.

3.7 Proactive Monitoring: Putting It All Together—One Approach

1. Establish a list of high-risk situations for which you wish to audit, referring to the list of threat use cases, and adding your own, where appropriate.
2. Assess not only the probability of occurrence of each situation, but also the impact of each instance of the situation, should it occur. Combining the probability with the impact, you may determine an expected consequence for each situation.
3. Prioritize your list according to the expected consequence of each situation.
4. For each high-consequence situation, assess the feasibility of actually doing audits for the situation:
    a. Do available logs already contain all the data elements necessary to audit for the situation?
    b. Are there reporting or analysis tools available to assemble and correlate the required data elements into meaningful audit reports on the situation?
    c. If there are gaps, can a specific plan be developed to close them, so that auditing for the situation may begin within a reasonable time?

4 Glossary

Electronic Health Record (EHR)
The clinical repository and/or ancillary systems designed to store and make available specified electronic PHI from the electronic health information systems of HICs to act as a single repository.

Consent Directive
Consent directive has the same meaning as in the *EHR Consent Management Policy* and its associated procedures, as amended from time to time.

Privacy Breach
Privacy Breach has the same meaning as in the *EHR Privacy Breach Management Policy* and its associated procedures, as amended from time to time.

Term or Acronym	Definition
HIC	Health Information Custodian
PHI	Personal Health Information, as defined in the *Personal Health Information Protection Act, 2004*
PHIPA	*Personal Health Information Protection Act, 2004*

5 References and Associated Documents

Electronic Health Record Logging and Auditing Policy and its associated procedures

Electronic Health Record Consent Management Policy and its associated procedures

Electronic Health Record Privacy Breach Management Policy and its associated procedures

eHealth Ontario Electronic Health Record Access Services Schedule

Alberta Health and Alberta Health Services, *An Overview of Alberta's Electronic Health Record Information System, Section 3e) Maintaining Alberta EHR Privacy and Security – Auditing Access by Users*. August 2013. Available online at http://www.albertanetcare.ca/documents/An_Overview_of_Albertas_ERHIS.pdf

American Health Information Management Association (AHIMA), *Privacy and Security Audits of Electronic Health Information*, Available online at http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_050599.hcsp?dDocName=bok1_050599

COACH *Guidelines for the Protection of Health Information Special Edition – Access Audits for Electronic Health Records*, 2014.

eHealth Ontario *Health Care Audit Event Implementation Guide v. 1.0, Available online at* http://www.ehealthontario.on.ca/en/standards/view/health-care-audit-event

Information and Privacy Commissioner of Ontario, *Detecting and Deterring Unauthorized Access to Personal Health Information* January 2015. Available online at https://www.ipc.on.ca/images/Resources/Detect_Deter.pdf.

International Standard Organization, *ISO 27789:2013 Health informatics - Audit trails for electronic health records*.

Information and Privacy Commissioner of Ontario, *PHIPA Order HO-010, 2014*. Available online at https://www.ipc.on.ca/images/Findings/ho-010.pdf

Information and Privacy Commissioner of Ontario, *PHIPA Order HO-013, 2014*. Available online at https://www.ipc.on.ca/images/Findings/ho-013.pdf

Manitoba eHealth*, Auditing EMR User Activity*. Available online at http://www.manitoba-ehealth.ca/commPhysicians/files/AuditingUserActivity.pdf

Province of Alberta, *Health Information Act, Alberta Electronic Health Records Regulation, section 6, logging capacity required and section 7. Audit of information logs* Available online at http://www.qp.alberta.ca/documents/Regs/2010_118.pdf