Provincial Logging and Auditing Standard v. 2.0

Primary and Preventative Health Services

Alberta

Provincial Logging and Auditing Standard v. 2.0 | Primary and Preventative Health Services
 | September 15, 2025 | ISBN XXX-X-XXXX-XXXX-X

Contents

1.0 Introduction

The *Health Information Act* (HIA) is intended to protect the privacy of individuals and the confidentiality of their health information, to ensure that health information is shared appropriately, and to ensure that health records are managed and protected properly.

The Provincial Logging and Auditing Standard (PLAS) identifies the legislated logging and auditing requirements for custodians within the Alberta health sector. These requirements are derived from the HIA and the *Alberta Electronic Health Record Regulation*. It also provides guidance for the logging of legislated data elements and provides examples of reports to be used in auditing of access to health information.

2.0 Scope

This standard applies to Primary and Preventative Health Services, and all custodians under the HIA, including Alberta Health Services (AHS), Covenant Health, and all community-based health services operated by a custodian.

Custodians, as defined in the HIA, are responsible for ensuring that appropriate logging and auditing controls are implemented in electronic systems or applications that collect, use, and/or disclose health information. The custodian may delegate these activities to an affiliate or to an information manager, but the custodian remains accountable.

2.1 Primary and Preventative Health Services is responsible to audit the Alberta Electronic Health Record (EHR) including the provision of on-demand access logs to support additional auditing or investigations by EHR authorized custodians or the Alberta Office of the Information and Privacy Commissioner (OIPC).

2.2 Systems or applications with users connecting to, contributing to, or otherwise interacting with the EHR, must work with Primary and Preventative Health Services Quality Assurance and Monitoring (QAM) to provide PLAS compliant access logs with details of the activity to the Primary and Preventative Health Services auditing data warehouse. Messaging transports and integration buses such as the Provincial Health Integration Exchange are used to “transfer user activity between systems or applications” and are outside the scope of PLAS.

2.3 Custodians of systems or applications are responsible to audit their systems or applications and may need to provide on-demand access logs to support additional auditing or investigations within the health sector.

2.4 Legacy systems or applications developed prior to the implementation of PLAS have historically been considered out-of-scope. However, pursuant to the HIA, custodians must take reasonable steps to maintain administrative, technical, and physical safeguards to protect health information in their custody or under their control.

> The OIPC has provided the guidance that within the context of the HIA and the *Alberta Electronic Health Record* ***Regulation*** (Alberta EHR Regulation), custodians must take reasonable steps to upgrade legacy health information systems or applications to address risks from non-compliance with the HIA.

3.0 Standard

3.1 Required Logging Capacity

Pursuant to *Alberta Electronic Health Record Regulation* section 6 an authorized custodian must ensure the system it uses to access the Alberta EHR creates and maintains logs containing the following information:

(a) user identification associated with an access;

(b) name of user and application that performs an access;

(c) role or job function(s) of user who performs an access;

(d) date of an access;

(e) time of an access;

(f) actions performed by a user during an access, including, without limitation, creating, viewing, editing and deleting information;

(g) One of more of the following:

(i) name of facility or organization at which the access is performed; or

(ii) name of the authorized custodian granting the user access to the Alberta EHR

(h) the type or class of health information accessed;

(i) unique identifier of the individual accessed;

(j) name of the individual accessed;

(k) any other information required by the Minister.

3.2 Implementation of Log Elements

Access logs must include complete information detailing user access to an individual's health information. The health information and individual accessed must be able to be identified or determined from the logs. Data elements must be logged each time an access and its associated action is performed on an individual's health information. All access to an individual's health information must be able to be displayed within user access and patient access reports used to facilitate audits of access to health information.

The data elements below are required to be logged each time health information is accessed. For clarification, "access" means an access of the Alberta EHR and information accessible via the Alberta EHR.

(a) User ID associated with an access

This is a unique identifier for a user. In the case of real-time or system-to-system communication, it should reflect user name if the action was initiated by a user. This data element must be logged for each access to an individual's record.

(b) Name of user or system/application that performs an access

This is the full name of the user accessing the individual's record. In the case of system-to-system or real-time communication it should reflect user name if the action was initiated by a user, or reflect system/application name if the action was initiated by a system/application. If it is possible to derive the name of the user or system/application that performs the access from the user ID (above), then this data element may not need to be logged.

(c) Role or job function(s) of user who performs an access

This refers to the profession or occupation of the user performing an access. For instance, physician, pharmacist, nurse, registered nurse, chiropractor, etc. This data element need only be logged for the first access of a unique session of access against an individual's record.

(d) Date of access

This refers to the day, month, and year of a user or system/application performing an access. This data element must be logged for each access to an individual's record.

(e) Time of access

This refers to the hour, minute, and second of a user or system/application performing an access. This data element must be logged for each access to an individual's record.

(f) Actions performed during an access

This refers to the actions performed by the user during an access and may include one or a combination of the following: create, view, update/modify, delete, patient search, copy, print, etc. This data element must be logged for each access to an individual's record.

The actions performed must be captured at a level that does not disclose patient care or treatment. For example, "Lab Test" is acceptable, "Hemoglobin A1c test" is not acceptable.

The EHR and connected systems or applications must capture unmasking or break-the-glass activity while ensuring health information is not disclosed.

(g) Name of facility, organization, or custodian provisioning access

This refers to the name of the facility/organization (legal entity) at which an access is performed; Custodian refers to the name of the authorized custodian who authorized the user to access the Alberta EHR. The name of the facility/organization must be unique and may not be shared among legal entities.

One data element, at minimum must be logged for each access to an individual's record. More data elements can be logged to provide greater granularity for audit and follow up purposes.

The EHR and connected systems or applications use the Wellnet Distributed Facility Identifier (WDFA) to meet the PLAS requirement for facility/organization name. The WDFA is also used during EHR auditing to support identification of the custodian(s) responsible for user access at a specific location.

(h) The type or class of health information accessed

This refers to a description of the health information that was the subject of the access or other action by the user. The specific information does not need to be captured rather the type or class of information. For example, lab test results, diagnostic image or dispense event.

(i) Unique identifier of individual accessed

This refers to the unique identifier of the individual whose information is being accessed. This data element must be logged for each access to an individual's record. Use of a Personal Health Number (PHN), Unique Lifetime Identifier (ULI), or Medical Record Number (MRN) must be displayed in audit reports to differentiate between individuals with same or similar names. If it is possible to derive the individual's name from the PHN without impacting the efficiency of the logging application then the name of the individual does not need to be logged.

(j) Name of the individual accessed

This refers to the unique identifier of the individual whose information is being accessed. This data element must be logged for each access to an individual's record. If it is possible to derive the name of the individual from the PHN without impacting the efficiency of the logging application then the name of the individual does not need to be logged.

3.3 Log Storage, Retention, and Access

Each custodian is responsible for the following:

- To determine, document, implement, and maintain an appropriate method for storing access log data.
- To determine, document, implement, and maintain appropriate security controls to protect logged data Including:
    - Restrict access to the access log data to only those with a need-to-know.
    - Protect access log data and reports from modification.

- Retain access logs for a period of 10 years following the date of the use (Refer to section 56.6(2) of the HIA. Refer to “Disclosure of Health Information” from the HIA Guidelines and Practices Manual, or to health profession codes of practice.)

3.4 Access Audits

Access to systems or applications that collect, use, and/or disclose health information must support reports required for on-demand auditing triggered by custodian or an individual’s request, breach investigations, and other privacy and security related investigations or concerns.

3.5 Auditor Support

The custodian must ensure any auditors of the system or application are provided the level of independence required for auditing and investigations, possess a sufficient understanding of system or application for the determination of appropriateness of access or determination of breach, and are provided with confidential communication channels to report findings in support of potential disciplinary actions or dismissal.

4.0 Audit Report Examples

When auditing systems or applications, custodians are free to use the example reports below, or to develop other reports specific to their systems or applications. The development of audit reports may need to consider the number of users accessing the information, the frequency of the access to the information, how often users or user permissions are granted/changed/revoked or verified, the volume of information held or accessed, the anticipated times of access to information, and any other factors as determined by the custodian.

4.1 Frequently Accessed Record Audit

This report generates information about an individual’s records that have been accessed several times within a specified period, and information about the users who accessed the records.

Objective	Identify users who access health information repeatedly within a specified period.
Example Scenario	Peter accessed Mary’s records 20 times within a period of one month. If, on review, it is determined that Peter’s accesses to Mary’s records have been inappropriate, additional information (what was accessed, how, when, by whom) can be gathered through supplementary reports, such as a Patient Activity report.
Sample Size	All individuals with a predetermined number of accesses. A threshold value is typically used to determine excessive usage.

4.2 Same User Same Patient Last Name Search Audit

This report generates a list of users who access the records of individuals who have same last names as them within a specified period, and information about the individuals whose records were accessed by the user.

Objective	Identify users who have accessed their own health record or the health record of a family member when not providing healthcare services.
Example Scenario	Peter Smith (user) accessed Kevin Smith's records 4 times and Bob Smith's records 3 times. The custodian discusses this with Peter to confirm a health care relationship, and if not satisfied, generates additional reports, e.g., Patient Activity Report, to determine what Peter accessed and when. These additional reports may indicate that the access goes further and may include family members with different last names, or co-workers.
Sample Size	All users, a random sample of users, or a target/defined group, such as new users to ensure training has taken place.

4.3 Unmasking Decision Audit

Alberta Netcare provides Global Person Level Masking functionality. The application of a mask against an individual's health information prevents the automatic display of information within that record. Authorized health service providers may unmask a record if necessary and where the provider has role-based permissions, but only in accordance with specific rules set out in the Alberta Netcare Terms of Use. Unmasking activity within Alberta Netcare is flagged, logged, and audited.

This report provides information about a user who unmasked and accessed an individual's record within a specified period.

Objective	Identify users who have unmasked and accessed an individual's record to assist in determining the appropriateness of the unmasking.
Example Scenario	Dr. Smith treats Patient X who has masking applied to their records. This results in Dr. Smith being identified in any UNMASK reports in audit reports, as Dr. Smith is unmasking records far more often than average.
Sample Size	All users who unmasked health information. A threshold value may be used to determine excessive usage.

4.4 Patient Activity Audit

This report provides detailed access against a particular individual within a specified period. This is from the individual's point of view. The report can also be used to facilitate breach investigation and/or an individual's access request.

Objective	Identify all accesses to the individual's personal health record.
Example Scenario	HIA legislation allows individuals to know who accessed their record; this audit must provide that information in a manner that facilitates the easy identification of the users who accessed an individual's health record, what they accessed, what they did, and from which location the access was made.
Sample Size	Limited to a specific individual.

4.5 User Activity Audit

This report provides detailed access activities of a user within a specified period. This audit report can facilitate breach investigation of a user as part of an investigation. It can be used to provide a more granular review of all actions performed by a user within the system or application. It may be matched with other audits or information (e.g., co-worker names) to determine appropriateness of access.

Objective	Support investigation of complaints regarding inappropriate use or disclosure of personal health information, reported either directly to custodian or to the OIPC.
Example Scenario	This audit must plainly indicate all actions performed by a user over a specified time period, including every individual's record accessed, and why.
Sample Size	Limited to a specific user.

4.6 Lack of Use Audit

This report generates a list of users who have been inactive within a specified period. Running this audit assists the custodian efforts to ensure former employees have had their access deleted.

Objective	Identify user accounts that may need to be disabled or to terminate users who have been inactive for an identified number of days.
Example Scenario	Assist custodians in their user review activities and identifies when additional actions such as user off-boarding were not correctly completed.
Sample Size	All inactive users.

4.7 Frequent Failed Login Audit

This report generates the number of failed login attempts for each user within a specified period. This audit may identify inappropriate access attempts by an account.

Objective	Identify users who have been locked out, have performed several failed login attempts, or attempts by an unauthorized user to guess an authorized user's login.
Example Scenario	The system login requirements track successful and unsuccessful logins. Any attempt to login that fails must have a reason. Legitimate reasons may include return to work after a period of absence, or immediately after a password change. Several failed attempts may indicate attempts to gain access without valid credentials. Also, the time period of the attempts should be noted. Attempts during non-work hours may indicate unauthorized attempts to login.
Sample Size	All users.

4.8 Log-in Time Audit

This report provides information about the times a user is logged into the system or application.

Objective	Identify users who are logged in during non-work hours, holidays etc.
Example Scenario	An employee is on maternity leave however her account is still being used. This may indicate unauthorized access and a compromised system.
Sample Size	All users.

4.9 User Activity and Billing

This report matches the user activity to the amount or type of billing submitted by the user or organization.

Objective	Confirm user activity is legitimate.
Example Scenario	This audit must indicate appropriate detail of actions performed by a user to allow a comparison to what was billed over a specified period.
Sample Size	Specific user, specific time period.

5.0 Linked Documents

Name	Location
Health Information Act	http://www.qp.alberta.ca/documents/Acts/H05.pdf
Alberta Electronic Health Record Regulation	http://www.qp.alberta.ca/documents/Regs/2010_118.pdf
HIA Guidelines and Practices Manual	https://open.alberta.ca/publications/9780778582922

6.0 Revision History

Version	Changes	Reviewers
1.0 (Nov 2007)	Initial Standard	IPC Unit, Provincial Logging and Audit Standard Working Group
1.1 (Jan 2008)	Revised Standard	AHW Architecture
1.2 (Sep 2009)	Approved Standard	ICA Unit, Alberta Health Services, IM/IT Strategic Planning Committee

1.3	(Nov 2012)	General Review	Alberta Health Privacy and Security Unit
1.4	(Mar - Sep 2019)	Update to clarify applicability of data elements, roles and systems, and addition of sample reports	Alberta Health Privacy and Security Team, Health Sector Security Committee
2.0	(January 2025)	Standard rewrite based on new approach to logging requirements.	Primary and Preventative Health Services Health System Cybersecurity & Privacy Operations