Yukon
Information
and Privacy
Commissioner

3162 Third Avenue, Main Floor
Whitehorse, Yukon, Y1A 1G3
T: 867.667.8468
F: 867.667.8469
1-800-661-0408 ext. 8468
www.yukonombudsman.ca

Guidance for logging and auditing of electronic systems containing personal information or personal health information

Access to Information and Protection of Privacy Act
Health Information Privacy and Management Act

January 25, 2022

Table of Contents

Terminology

ATIPPA means the *Access to Information and Protection of Privacy Act*, SY 2018.

ATIPPA Regulation means the *Access to Information and Protection of Privacy Regulation*, O.I.C. 2021/25.

Auditing means the process of formally examining records (logs) to investigate confidentiality and integrity of personal information or personal health information.

Collusion means an agreement between people to act together in order to circumvent controls and act contrary to policy or rules protecting personal information or personal health information.

Custodian has the same meaning as in the *Health Information Privacy and Management Act.*

HIPMA means the *Health Information Privacy and Management Act.*

Information Security Management System means a set of policies, standards and procedures for systematically managing and protecting an organization's sensitive data.

Logging means the creation of a non-repudiable record regarding access to, creation of, addition to, alteration of, or deletion of personal information or personal health information.

Non-repudiation in relation to logging and auditing means creating assurance that a record is proof of a course of action, i.e., it cannot be repudiated or shown to be invalid.

Personal health information (PHI) has the same meaning as in HIPMA.

Personal information (PI) has the same meaning as in ATIPPA.

Policy means a formally established requirement ratified by senior management.

Procedure means an operational process to achieve compliance with a policy by means of achieving expectations as set out in a standard.

Public body has the same meaning as in ATIPPA.

Standard means objective, quantifiable, and measurable expectation regarding the implementation of a policy.

Obligation to audit

If you are a public body or a custodian, you have an obligation to perform logging and auditing on your electronic systems that contain personal information (PI) or personal health information (PHI).

For custodians, this obligation is set out in HIPMA, subsection 22 (3).

> *A custodian must create and maintain, or cause to be created and maintained, for any electronic information system the custodian uses to maintain personal health information, a record of user activity that includes, in respect of each incident of access by a person, through the system, to personal health information or personal information.*
>
> *(a) the person's user identification;*
>
> *(b) the date and time of the incident;*
>
> *(c) a description of the information that is accessed or that could have been accessed; and*
>
> *(d) any prescribed information.*

For public bodies, this obligation is set out in ATIPPA General Regulation 9, subsections 10 and 11.

> *(10) Subject to subsection (11), the head of a public body must ensure that a record of user activity is maintained in respect of each instance when an employee of the public body accesses personal information in an electronic information system maintained by the public body.*
>
> *(11) Subsection (10) does not apply in respect of an electronic information system obtained by a public body before the coming into force of that subsection.*

Regardless of Regulation 9, subsection 11, to create assurance that records containing PI are not viewed arbitrarily or altered accidentally or maliciously, logging and auditing for any electronic system are a necessity.

Purpose of logging and auditing

Logging ensures that a record is created of any user activity within information systems. If properly done, these logs can be used to prove or disprove what users of the system did or did not do. This specific type of assurance regarding logs is referred to as non-repudiation. The process by which that course of action is assessed is called auditing. Auditing can be performed reactively or proactively. A proactive audit regularly and continuously analyzes logs for any deviation of agreed

upon behaviour by users of the system. A reactive audit takes place after an incident or suspicion of an incident.

A secondary but no less important aspect of logging and auditing is that they serve as a deterrent against improper behaviour where the requirements for this activity are embedded in policy and procedure. Users who are trained on the policy and procedure are notified that their actions on the system are being logged and audited. Knowledge of this fact reduces the likelihood that they will engage in unauthorized behaviour, such as snooping (accessing PI or PHI for personal reasons), because they know it will be detected and addressed. See the section "Governance to ensure effective auditing" below, for more information about logging and auditing policy and procedure.

Requirements for logs

To be able to perform audits reliably and accurately, logging must comply with the following requirements.

1. There must be assurance of the authenticity of users that log on to the system and thus create logs. To ensure this, strong authentication[1] must be used. No multi-user or generic accounts can be used, and unique usernames are a requirement. Users must be trained not to share their account information and not to use another person's account at any time.

2. The right information must be logged. Logs must contain sufficient information to establish what events occurred, when they occurred, and who (or what) caused them. Some examples of the necessary information include logging time stamps, usernames, object(s)/record(s) involved, and the operation carried out (for example, access, view, move, edit, print, remove, export, etc). There must be assurance that all such actions are logged. If administrative or technical changes take place, a review of the logging process should be triggered to ensure the right data points are still being captured.

3. Logs must be stored for an appropriate amount of time, taking into account legal and operational requirements. Logs typically contain PI regarding the users of the system and, depending on the level of detail in the logs, may also contain some PI of the records stored in the system (for example, employee X viewed patient Y's record). Because there are privacy risks associated with the lengthy retention of PI that is not being used for service delivery, logs should only be stored as long as they are needed to serve their specified purpose and as required by law.

[1] Some form of multi-factor authentication is currently considered the standard for systems containing PI or PHI.

4. Access to logs must be restricted to only those persons who have a legitimate need to access them. Usually, no one needs direct access to logs, since access to them should occur via audit tools that facilitate viewing the logs without altering them. Raw log files should be configured to be "read only", so that no alteration of the logs takes place. Logs should be included in backup and restore routines, so that in the event of an incident, they can be recovered.[2]

5. Any notice requirements set out in law for collection of PI that takes place as part of creating logs must be met.

Requirements for audits

1. Ensure administrators are trained and are provided with the proper tools and necessary resources to effectively audit. This may include acquiring tools to help make sense of log files, if the tools are not available in the system itself. It also includes training on using auditing policy, standard, and procedure. The section below on governance provides a primer on these matters.

2. Ensure access to auditing tools is limited to authorized individuals trained to only use the tool as needed. This is because, depending on the type of tool used, they may reveal PI.

3. Ensure the auditor is impartial and has no conflict of interest.

4. Use rotation of duties between auditors or work with a two-auditor system to reduce the chance of collusion.

5. Periodically evaluate the audit process for effectiveness, compliance with regulatory changes, and adherence to vendor (system) and industry best practices.

Governance to ensure effective auditing

For logging and auditing to be conducted effectively, a **policy, standard** and **procedure** should be used.

a. The logging and auditing **policy** statement contains confirmation that logging and auditing of information systems containing PI and/or PHI must take place and who is responsible for the implementation of the policy. This policy statement may be included in a broader policy framework such as an information security management system.

[2] It is common for hackers and malware alike to attempt to wipe any logs to make forensic analysis of an attack harder or impossible to conduct.

b. The logging and audit **standard** ensures objective, quantifiable, and measurable expectations are set regarding the implementation of a policy. It defines the requirements of logging and auditing (what, who, when, how). It also defines what triggers an incident as a result of finding unauthorized behaviour via the audit. It may define the incident response or link to a separate standard for that purpose. Some elements that may be addressed by the standard are as follows.

    i. What information should logs contain?

    ii. Is the auditing incident-based, random or structural? For incident-based and random audits, risks should be recorded and reported as part of information security risk management practices.

    iii. What is unauthorized or anomalous behavior? This may link back to other policies or agreements e.g., authorized and acceptable use of information technology policy, privacy policy, etc.

    iv. How is such behaviour investigated? There may be a need to determine the cause of the anomaly visible in the logs and as reported in the audit. E.g. Someone could be snooping; an account could be compromised; or technical controls (that should have limited any access in the first place) may have failed.

    v. What actions are triggered as the result of the investigation? These could be sanctions such as revocations of access, administrative leave, or steps such as adjustment of technical and administrative controls, further investigation into a compromised account, etc.

c. The logging and audit **procedure** defines the specifics of conducting an audit that will be performed. Some elements that may be addressed by the procedure are:

    i. who it will be reported to;

    ii. when the audit trail (results) will be reviewed;

    iii. who is responsible for reviewing the audit trail;

    iv. how employees will be informed of consequences if the audit trail reveals unauthorized activity;

    v. how anomaly detection will be handled and how an incident will be created and reported;

vi. what steps to perform to do the audit, i.e., practical step-by-step administrative guidance; and

vii. where and how audits are documented.

Considerations regarding email and records management systems

Under HIPMA, custodians must create logs "…for any electronic information system the custodian uses…"[3]. This definition includes email systems and for good reason. Email boxes are often poorly managed and, because of that, may contain astonishing amounts of information and, in the case of custodians, PHI. The most used email product (MS Exchange, also known as Outlook) can audit access to email accounts. However, it does not currently support effective logging on a per record basis for mailbox owners.

If such account level auditing is not in place, a custodian may not be able to detect unauthorized access to an email account when, for example, a password is compromised. If they do detect unauthorized access but do not have record level (individual email in this case) logging enabled, there is no way to tell which records were or were not accessed. Record level access logging enables a custodian to limit the breach to only the items accessed. As this type of logging is currently not supported by Outlook[4]**, email should not be used as a records management system.** Since there is no way of knowing which information was viewed by the unauthorized person, all information in the account is considered to have been accessed or disclosed without authorization and is considered to be part of the breach.

In practice, logging and auditing in **a properly designed and set up records management system** limits breaches significantly, since it becomes clear which select items were accessed. **This greatly reduces the amount of work, costs and liabilities resulting from a breach**.

The same scenario holds true for records management systems, electronic medical records systems, and similar systems holding PI or PHI. However, modern software for these purposes should have logging enabled by default. Still, to be able to detect breaches and limit their impact, regular auditing and/or automated audit reports on anomalous behaviour are required. If you are already using such a system, ensure proper logging and auditing actually takes place.

[3] Subsection 22 (3) of HIPMA.

[4] There is third party software available, such as Solarwind's Exchange Auditing Software, which does allow logging and auditing of individual records in email boxes; however, third party software comes with its own risks and should not be a replacement for proper information management i.e., not using email as a records management system.

More information

For more guidance on developing, implementing, and maintaining effective log management practices throughout an organisation, see the link below.

https://csrc.nist.gov/publications/detail/sp/800-92/final

Contact us

Phone: 867-667-8468
Tollfree in the Yukon: 1-800-661-0408 (ext. 8468)
Email: info@yukonombudsman.ca

Disclaimer

The purpose of this document is to inform custodians and public bodies about the requirements to use logging and auditing and to support them in meeting their privacy and security obligations under HIPMA and ATIPPA.

This document is not intended as, nor is it a substitute for, legal advice. For the exact wording and interpretation of HIPMA and ATIPPA, please read the Acts and regulations in their entirety. This document is not binding on Yukon's Information and Privacy Commissioner.