

Personal Injury Law and Practice 2025

Audit trails and privacy protection in medical malpractice cases

October 7, 2025

Ryan Marinacci
Bogoroch & Associates LLP



Agenda

- Patient's right to information about medical condition and treatment
- Understanding Electronic Health Record (EHR) systems
- Privacy legislation and consent
- What audit trails can reveal and conceal
- Practical examples and recent case law
- Implications for litigation practice

- *McInerney v. MacDonald*, 1992 CanLII 57 (SCC) (La Forest J):
...information about oneself revealed to a doctor acting in a professional capacity remains, in a fundamental sense, one's own. The doctor's position is one of trust and confidence. The information conveyed is held in a fashion somewhat akin to a trust. While the doctor is the owner of the actual record, the information is to be used by the physician for the benefit of the patient. The confiding of the information to the physician for medical purposes gives rise to an expectation that the patient's interest in and control of the information will continue.

What is an Electronic Health Record System?

- A digital record of an individual's medical history that can be shared electronically by authorized health care providers
- May include clinical data, test results, notes, administrative data, communication between providers, notification systems, metadata
- Connects to eHealth Ontario data sources (HRM, OLIS, eConsult, DHDR, etc.)
- Examples:
 - Electronic health record (EHR): Epic Systems, MEDITECH, Oracle Cerner
 - Electronic medical record (EMR): TELUS Health Solutions (CHR, Med Access, PS Suite)

Understanding electronic health record systems

What else can they contain?

- Data from electronic monitoring equipment
- Scheduling, alarms and reminders
- Patient-facing records
- Electronic messaging tools
- Shared information from external data sources (ClinicalConnect, OLIS, HRM)
- Integration with other information management tools (Picis Anesthesia Manager)

Provincial privacy laws

- The right to privacy in Ontario is governed by several pieces of legislation. The applicable legislation is context-specific
- The *Personal Health Information Protection Act, 2004 (PHIPA)* governs the collection, use and disclosure of personal health information in Ontario
- The *Freedom of Information and Protection of Privacy Act (FIPPA)* applies to Ontario's provincial ministries, agencies, boards, commissions, hospitals, universities and outpatient healthcare services (LHINs)
- The *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)* governs protection and access to information held by municipal institutions, including transit commissions and police service boards

PHIPA, 2004 – Access to personal health information

- Part IV - Collection, Use And Disclosure of Personal Health Information

Section 29 Requirement for Consent

29 A health information custodian shall not collect, use or disclose personal health information about an individual unless,

(a) it has the individual's consent under this Act and the collection, use or disclosure, as the case may be, to the best of the custodian's knowledge, is necessary for a lawful purpose; or

(b) the collection, use or disclosure, as the case may be, is permitted or required by this Act.

Consent, use and disclosure

- When is consent required?
 - Consent for treatment vs consent for other use
 - Implied vs express consent
- Use of personal health information limited to intended purpose
- Privacy rights are not waived by filing a lawsuit
- Right to privacy continues after death
- Custodians are obligated to notify individuals in case of unauthorized access (e.g. security breaches)

PHIPA, 2004 – Examples of permitted uses

- For providing health care
- For risk management, error management or quality improvement
- For educating agents
- For research
- For planning and delivering programs

PHIPA, 2004 – Security

- Section 12(1):

A health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal.

Audit trails

What are they?

- An audit log can contain every instance an electronic record was viewed, handled, modified, or otherwise dealt with
- This includes:
 - The type of information that was accessed
 - The date and time of record access
 - The identity of the person accessing the record

Audit trails

Why do they matter?

- Establishing *what* a healthcare provider reviewed and *when*
- Determining when records were created, modified or deleted
- Evidence of compliance or non-compliance with privacy rules and policies

Audit trails

Can Reveal

Exact timing of access/modifications

Whether notes were back-dated or altered after the fact

Who accessed a record after the therapeutic relationship ended

Patterns of access suggesting policy breaches

Can Conceal

Information may be limited by system design

Logs may omit details like location, terminal ID, role of individual

Gaps in logging, missing metadata, or deleted logs

Use of shared credentials

Audit trails and *PHIPA*

- Audit trails are “personal health information” under *PHIPA* s. 4 (see e.g. *PHIPA* Decision 159, 2021: “each of the audit reports, therefore, is a record of personal health information relating to the patient in question”)
- Patients have rights of access to their personal health information, including logs of access/modification
- Health information custodians must protect personal health information, limit access, maintain reasonable safeguards
- Obligations for custodians to respond to access requests within 30 days
- Employee names cannot be redacted (*PHIPA* Decision 152, 2021)
- Other relevant rules include CPSO and CNO policies; hospital privacy policies

The importance of audit trails - Hospital privacy breaches

- Improper access by Nurse to 11,000 patient files over ten-year period to steal Percocet (*Stewart v Demme*, 2022 ONSC 1790)
- Access to hospital records of up to 26,000 persons by three rogue employees to sell Registered Education Savings Plans (*Broutzas v Rouge Valley Health System*, 2023 ONSC 540)
- Targeted searches of up to 846 newborn males to offer circumcision services by physician and clinic (*PHIPA* Decision 298, August 17, 2025)
- Emergency physician accessed hospital chart of motor vehicle accident patient, resulting in referral to his wife, a personal injury lawyer (*PHIPA* Decision 147, June 18, 2021)
- Emergency physician received 4-month suspension for unauthorized access to 710 patient charts (*CPSO v Zhang*, 2025 ONPSDT 1)

Audit trails in civil litigation

- When was information accessed?
- Was information ever accessed?
- When was a note created and signed?
- Was a note modified?
- Was a note deleted?
- Was a note accessed after the end of patient care?

Audit trails in civil litigation

Plaintiffs' Motion in *Law v Preiner*

- Surgical malpractice case involving patient death
- Plaintiffs requested full audit trails from Defendant Hospital from preoperative period to after death
- Hospital refused to produce logs after date of death on the basis of relevance
- Plaintiffs argued that accessing medical records after death was relevant to allegations concerning breach of hospital policies

Audit trails in civil litigation

Endorsement of Associate Justice Brott in *Law v Preiner*:

“The defendant asserts that the plaintiff is on a fishing expedition. She outlines the sole issue in the action as whether the care provider caused the death of Ms. Law and accordingly submits that the only material time in issue in the action is the time when the deceased was a patient in the hospital. In her view, if there was a breach of patient privacy, the only relevant time to look at, is for the period between September 3 to November 6.”



Audit trails in civil litigation

Endorsement of Associate Justice Brott in *Law v Preiner*:

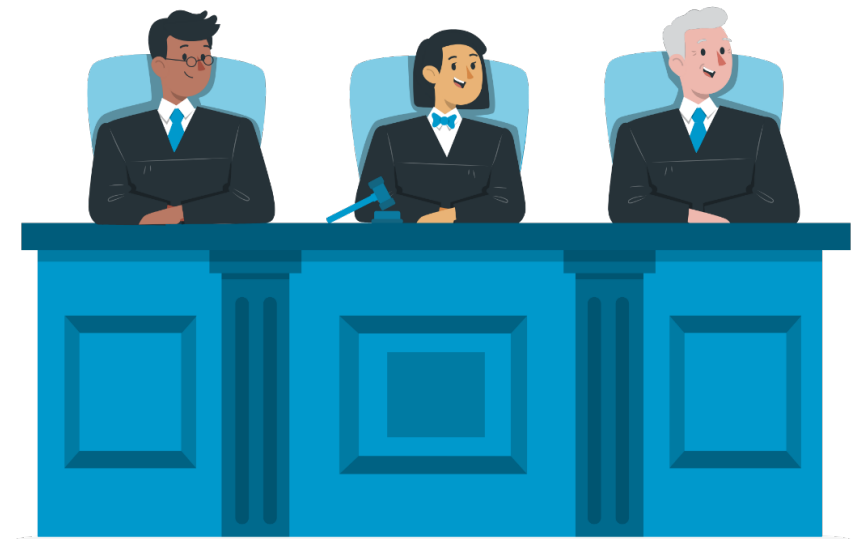
“In my view, if the hospital accessed the patient records even after the death of Ms. Law then those actions go to the alleged breach of patient privacy. The breach of the policies of patient privacy have been clearly pleaded. The policies around patient privacy do not end with the death of a patient. Accordingly, I find that the audit reports for the period from November 7, 2021 to the present are relevant and producible.”



Audit trails in administrative proceedings

The Estate of Richard Martin v. HPARB, 2023 ONSC 2993

- Civil suit against several physicians regarding failure to diagnose compartment syndrome
- Audit trails produced in the litigation revealed a defendant physician had accessed the plaintiff's medical records several times over the following four years
- Plaintiff's counsel filed a complaint to the CPSO regarding the physician's conduct
- Complaint dismissed by the ICRC → appealed to HPARB → judicial review by Div Court → remitted to HPARB → returned to CPSO



Patient privacy concerns in civil litigation

- Defence Counsel removed as solicitor of record for directly contacting Plaintiff's treating physician (*Smith et al. v Muir*, 2020 ONSC 1118)
- Defence causation expert agreed it "was an inappropriate exercise of his position" to access private patient records of four patients to corroborate his opinions (*Campbell v Roberts*, 2014 ONSC 5922)
- Plaintiffs argued treating OT breached *PHIPA* by speaking with Defence Counsel in preparation for trial (*Ibrahimova v Cavanagh*, 2025 ONSC 4808)
- Defence motion for production of in-home video recordings dismissed (*Ibrahimova et al. v Cavanagh et al.*, 2025 ONSC 1152)

Thank you