Confidentiality and Privacy — Personal Health Information

Table of Contents

The College of Nurses of Ontario's (CNO) practice standards outline accountabilities for nurses and inform the public, including clients and organizations, what to expect of nurses. The standards apply to all nurses regardless of their role, job description or area of practice. Nurses are expected to practice in compliance with relevant legislation, the *Code of Conduct*, all other standards of practice of the profession and applicable employer and organizational policies. Not complying with legislation or failing to meet the standards of practice may be considered **professional misconduct.**

Introduction

A therapeutic nurse-client relationship is essential to the **clients'** health and well-being and is grounded in trust, respect and empathy. One way that nurses can build a nurse-client relationships based on trust is by respecting clients' rights around confidentiality and privacy. Nurses have professional and legal obligations to maintain the confidentiality and privacy of client **personal health information**.

This standard outlines nurses' accountabilities for safeguarding clients' personal health information in accordance with privacy legislation. Although this standard focuses on the *Personal Health Information Protection Act, 2004* (PHIPA) requirements, nurses should be aware that other legislation may also apply depending on their role, area of practice or setting. These may include, but are not limited to, the *Freedom of Information and Protection of Privacy Act, 1990*, the *Personal Information Protection and Electronic Documents Act*, the *Regulated Health Professions Act, 1991* (RHPA), the *Quality of Care Information Protection Act, 2016*, the *Substitute Decisions Act, 1992* and other sector-specific legislation.

Nurses must ensure there is transparency in how client personal health information is accessed, collected, used and disclosed. As technologies continue to evolve, nurses are required to continue to meet confidentiality and privacy requirements regardless of the format or platform used to manage a client's personal health information. This includes technologies such as email, text or instant messaging, telephone, **artificial intelligence** (AI) tools, video or audio conferencing, fax and internet. See CNO's ***Virtual Care*** practice guideline and *Artificial intelligence in nursing practice* guidance and educational tool for more information.

Bolded terms are defined in the glossary at the end of the document.

To meet the expectations for this practice standard, nurses must consider the following personal health information principles:

	Access Nurses facilitate access to personal health information as required. When authorized, nurses access information only for the intended purposes to promote safe and quality care.
	Collection Nurses gather, acquire, receive or obtain only as much personal health information as necessary for the specific purpose of the collection.
	Use Nurses handle or deal with personal health information only for the intended purposes.
	Disclosure Nurses meet legal and professional accountabilities when making personal health information available or releasing it to another custodian or person.

Each principle includes a set of nursing accountabilities, which are described in this standard.

Personal Health Information

As outlined in PHIPA [ss 4(1)], personal health information is any **identifying information** about an **individual** that is in verbal, written or electronic form if the information relates to:

- the physical or mental health of an individual, including family health history
- the provision of health care to an individual (including the identity of the health care provider providing care to the individual)
- a plan that outlines the home and community care services to be provided by a health care provider or Ontario Health team, funded under section 21 of the *Connecting Care Act, 2019*
- payments, eligibility for health care or eligibility for coverage for health care
- the donation of body parts or substances (for example, blood), or information gained from testing these body parts or substances
- the individual's health number (for example, Ontario Health Insurance Plan (OHIP) number)
- the identity of an individual's **substitute decision-maker**
- the individual's digital health identifier or other identifying information related to the creation of the digital health identifier.

Clients do not have to be named for information to be considered personal health information. Information is "identifying" if a person can be recognized from it, or when it can be combined with other information to identify a person. When a **record** includes any personal health information, the entire record must be managed in accordance with personal health information legislation. This includes when a record contains both personal health information and other **personal information**, which is known as a mixed record.

The Personal Health Information Protection Act

PHIPA establishes rules for the management of personal health information, including its access, **collection**, **use** and **disclosure**, and outlines the client's rights regarding their personal health information in Ontario.

PHIPA also describes accountabilities related to **data minimization**. Data minimization refers to the collection, use and disclosure of only the personal information reasonably necessary to meet the purposes of the collection, use or disclosure, as the case may be [PHIPA, ss 30(2)].

PHIPA requires that personal health information be kept confidential and secure. PHIPA balances a client's right to **information privacy** with the need of health care providers and organizations providing health care to access and share health information.

PHIPA outlines two key roles:

Health information custodian

A person or organization listed in PHIPA that, as a result of their power or duties or work set out in PHIPA, has custody or control of personal health information [**Information Privacy Commissioner of Ontario** (IPC), September 2015]. This can include individuals providing care. **Health information custodians** (HICs) are responsible for:

a. developing, implementing, maintaining and monitoring practices and policies that ensure the confidentiality and **security** of personal health information
b. ensuring that records are retained, transferred and disposed of in a secure manner that follows prescribed requirements
c. complying with and ensuring that all **agents** are informed of their duties under PHIPA

Agent

Any person who is authorized by a HIC to carry out services or activities involving personal health information on the HIC's behalf and for the HIC's purposes (IPC, September 2015). This can include nurses who are employees, volunteers or contracted or credentialed by health care organizations (for example, clinics, laboratories, home and community care providers, hospitals, long-term care facilities, retirement homes and online telehealth platforms). Agents are responsible for:

a. complying with PHIPA and only using the information for the purposes they identified when requesting it from the HIC
b. notifying the HIC if personal health information is stolen, lost or accessed by unauthorised persons

Self-employed nurses

Nurses who are **self-employed**, (see CNO's *Independent Practice* guideline), or those employed in health services in non-health care settings (for example, school nurses) may be considered HICs rather than agents. Nurses acting as HICs are responsible for:

- designating a contact person, if they are not performing this function, to facilitate compliance with PHIPA and to respond to requests, inquiries and complaints from the public (PHIPA, s 15)
- posting a physical notice within the clinical environment or an electronic notice on their website that generally describes their information practices, how to reach the contact person, the process for accessing records or requesting corrections and the complaint process for clients (PHIPA, s 16)
- developing policies and procedures related to personal health information
- ensuring information practices comply with PHIPA and its regulations
- ensuring information is accurate, complete and up to date

- ensuring information is retained, transferred and disposed of securely

More information related to accountabilities of HICs can be found in the Partners in Safety section.

Personal health information belongs to the client

PHIPA recognizes that personal health information belongs to clients and the HIC simply has custody and control of the record. Capable clients, including a child who is less than 16 years of age, have the right to give, limit, refuse or withdraw their consent to the access, collection, use and disclosure of their personal health information. If there is a conflict between a capable child and the child's substitute decision-maker, the decision of the child to give, withhold or withdraw consent or provide information prevails [PHIPA, ss 23(3)].

Clients have the right to instruct that a part of their personal health information is not shared with other providers. This is a **consent directive**, commonly referred to as a **lockbox** provision. If a client instructs a nurse not to release a part of their health information to another practitioner, the nurse must advise the practitioner that some relevant information is incomplete or has been withheld at the direction of the client [PHIPA, ss 38(2)]. Employer/organizational lockbox policies and procedures should outline the roles and responsibilities of staff to facilitate lockbox requests. Locked personal health information may be disclosed when the HIC believes, on reasonable grounds, that disclosure is necessary to eliminate or reduce a significant risk of serious bodily harm to an individual or a group. Additionally, a lockbox cannot impede a HIC from recording personal health information about an individual that is required by law or by established standards of professional or institutional practice (IPC, September 2015).

If a client is incapable of consenting to the access, collection, use or disclosure of personal health information by a HIC, a substitute decision-maker may give, withhold or withdraw consent on behalf of the individual. Rules for who may act as a substitute decision-maker are similar to those in the *Health Care Consent Act, 1996*. See CNO's *Consent* guideline for more information, including the hierarchy of substitute decision makers. PHIPA also contains directions for substitute decision-makers when considering decisions relating to consent, appeal routes (for example, the Consent and Capacity Board) for clients found incapable and ways to deal with conflicts between people acting as client representatives.

Clients' right to access their personal health information

Under PHIPA, clients have a right to access their personal health information. There are specific situations where this access may be refused. Possible grounds in PHIPA for refusing client access to their own personal health information include:

- records that contain **quality of care information** [ss 51(1)]
- personal health information required for quality assurance programs [ss 51(1)]
- raw data from standardized psychological tests or assessments [ss 51(1)]
- when access to the information may present a risk of serious harm to the treatment or recovery of the client, or of serious bodily harm to another person [ss 52(1)]
- when access to the information would reveal the identity of a confidential source of information or reveal the identity of a person who was required by law to provide information [ss 52(1)].

When an exception applies, the client must be given access to any part of the record that can reasonably be separated from the information they are not permitted to access (IPC, 2015 September).

Clients also have the right to correct their personal health information. This means clients can request changes if they believe the record is inaccurate or incomplete. Requests for corrections can be made verbally or in writing. Ontario's health privacy law allows a HIC to correct the client's health records in response to an informal, oral request; but they can ask the client to submit the request in writing (IPC, n.d.-b). Clients can only

request corrections to their information if access has been provided. They may not restrict the access, collection, use or disclosure of their personal health information that is required by law or professional standards.

Client requests to correct personal health information may be refused in the following circumstances:

- the request is frivolous, vexatious or made in bad faith [PHIPA, ss 55(6)]
- the HIC did not create the record and does not have sufficient knowledge, expertise or authority to make the correction [PHIPA, ss 55(9)]
- the information is a professional opinion or observation made in good faith [PHIPA, ss 55(9)].

HICs must respond to access requests as soon as possible, but no later than 30 days after receiving a request. An extension of up to a maximum additional 30 calendar days is permitted if responding within the initial period would unreasonably interfere with the HIC's operations or if necessary consultations make a timely response impractical [PHIPA, ss 55(3)].

Further specific procedures for handling access and correction requests are outlined in PHIPA. Clients can file a complaint to an organization's contact person or to the Information and Privacy Commissioner of Ontario (IPC) about refusals to access requests or other breaches of PHIPA.

Access

Under PHIPA, nurses may access a client's personal health information only when it is necessary for providing or assisting in the client's care, or when required to carry out their authorized duties. Although this information may be easily accessible within the care environment, nurses are not permitted to view or use it for any reason outside of their professional duties (Canadian Nurses Protective Society, 2021). **Unauthorized access** or "snooping" includes the access, collection, use or disclosure of personal health information without the consent of the clients and for purposes that are not permitted or required (IPC, n.d.-d). Any unauthorized or inappropriate access to a client's personal health information is considered a privacy breach, which may result in a **report** being sent to CNO and/or the IPC. The IPC can issue administrative monetary penalties to both individuals and organizations when there has been a violation of PHIPA. In addition, violations of PHIPA prosecuted as provincial offences may result in court-imposed fines and/or other penalties as permitted by law.

Accountabilities

To uphold the principle of access, nurses must:

- ensure clients or substitute decision-makers know who on the **health care team** can access their information and how that information will be shared among health care team members, including information collected through technology platforms
- only access client health records:
    - to provide care or for authorized duties (for example, not using "hover to discover")
    - at the times required to provide that care or carry out authorized duties
    - through appropriate means, including on shared electronic health record systems (for example, Connecting Ontario or Clinical Connect)
- inform clients about their right to access information about their care, including processes or steps to obtain that information
- inform other health care providers when they are receiving incomplete health records (for example, when there is a lockbox)
- maintain confidentiality for the duration of the nurse-client relationship and after the relationship ends, including after a client's death
- comply with employer/organizational policies related to access, including use of approved devices and platforms
- ensure personal health information is safeguarded against theft, loss, unauthorized access, use or modification, including when using technology (for example, logging out of electronic health records or ensuring records are not left unattended).

Collection

PHIPA defines collection as the gathering, acquiring, receiving or obtaining of personal health information (PHIPA, s 2).

Collection may be done by members of the health care team. The health care team includes everyone providing care to the client, regardless of whether they are employed by the same organization. The Information Privacy Commissioner (August 2015), uses the term "circle of care" to describe the ability of a HIC to assume a client's implied consent to the collection, use or disclosure of their personal health information for the purpose of providing health care. PHIPA does not use the term "circle of care", instead it specifies the specific conditions that must be met to assume a client's implied consent to the collection, use or discloser of their information. [PHIPA, ss 20(2)]. It is a HIC's obligation to fulfil these conditions. One way a HIC may choose to fulfil their obligation is by posting a physical notice within the clinical environment or an electronic notice on their website that describes the purposes for the access, collection, use and disclosure of personal health information.

Under PHIPA, consent is generally required for the collection of a client's personal health information, unless implied consent requirements are fulfilled (IPC, September 2015). A HIC who receives personal health information from the client, their substitute decision-maker or another HIC for the purpose of providing or assisting in the provision of health care to the client is entitled to assume that it has the client's implied consent to collect, use or disclose the information for the purposes of providing or assisting in providing health care to the client, unless the HIC that receives the information is aware that the client has expressly withheld or withdrawn the consent [PHIPA, ss 20(2)].

PHIPA lists conditions that permit **indirect collection** of personal health information. Indirect collection is the collection of personal health information from someone other than the client, with or without consent. Information may be collected indirectly without consent when the client cannot provide it (for example, they are unconscious), if there is a question as to the accuracy of the information provided by the client, or when obtaining consent would affect the timeliness of care.

Accountabilities

To uphold the principle of collection, nurses must:

- obtain consent to collect personal health information from the client or substitute decision-maker, unless PHIPA allows collection without consent or indirect collection
- collect personal health information directly from the client or substitute decision-maker, unless PHIPA allows indirect collection
- collect only the personal health information that is needed to plan and provide care
- ensure confidentiality during the collection and storage of personal health information, whether in hard copy or electronic form (for example, email or instant messaging)
- comply with employer/organizational policies related to collection, including using only approved devices and platforms
- inform the client on the type of personal health information being collected through technology platforms, whether it will be recorded and where it will be stored
- obtain and document client's **express consent** prior to taking photographs, videos or recordings.

Use

In PHIPA, **use** means to handle or deal with personal health information in the custody or under the control of a HIC (PHIPA, s 2). Sharing information among members of the health care team to facilitate care is one use of information under PHIPA.

Nurses should collaborate with clients and any person or community the client wants involved in their care, as per the *Code of Conduct*. For example, the health care team may include cultural service providers such as Traditional Wellness Practitioners, Nutritional Healers, Medicine Persons and other religious or spiritual care providers.

Accountabilities

To uphold the principle of disclosure, nurses must:

- only use a client's personal health information for the purpose that it was originally collected, such as to inform and support the client's care plan, and not for purposes beyond which the information was originally collected. This includes information collected from shared systems (for example, Connecting Ontario or Clinical Connect)
- ensure confidentiality during the transmission, transfer and/or disposal of personal health information in any format (hard copy or electronic form)
- follow employer/organizational policies for use of personal health information, shared systems, approved devices and technologies, secure communication methods and record retention
- inform clients or substitute decision-makers when information may be used for purposes other than client care (for example, quality improvement or research, subject to restrictions and conditions)
- use technologies that meet legislative and employer/organizational policies and procedures
- maintain clients' privacy on **social media** and never share client information without **informed consent**
- use their knowledge, skill and judgment when evaluating risks, benefits, appropriateness and accuracy of using AI technologies.

Disclosure

Disclosure is defined as making information available or releasing it to another HIC or person. Clients have the right to withhold or withdraw consent to the disclosure of their personal health information or personal information.

Express consent for the collection, use and/or disclosure of personal health information or personal information is required in certain situations, for example, where the information is being:

- disclosed outside of the health care team (for example, submitting personal health information on an insurance claim)
- disclosed within the health care team for purposes other than providing or supporting care
- collected, used or disclosed for fundraising (though contact information can be provided without express consent) (PHIPA, s 32)
- collected, used or disclosed for marketing or marketing research activities (PHIPA, s 33).

Clients may give express consent verbally or in written form, and PHIPA does not require that it be in any specific format. Nurses should document when express consent has been obtained.

Disclosure without consent

PHIPA includes conditions that permit a HIC to disclose personal health information without the consent of the client. Some of these conditions include:

- if the information is reasonably necessary to provide health care and consent cannot be obtained in a timely manner, unless the client has expressly asked that it not be shared
- if contacting a relative, friend or potential substitute decision-maker for an individual who is injured, incapacitated or ill and unable to give consent personally
- if the HIC is a facility providing health care, and the facility is confirming that an individual is a client or resident of the facility, their general health status (for example, critical, poor, fair, stable) and their location in the facility, where the client has been given (at the earliest reasonable opportunity after admission) the option to object to such disclosure and has not done so
- if required to eliminate or reduce a significant risk of serious bodily harm to an individual or group
- to the Public Guardian and Trustee, a children's aid society and the Children's Lawyer for the purpose of carrying out their statutory functions
- as required for legal proceedings
- if permitted for the purpose of research, subject to restrictions and conditions [see PHIPA, ss 44(1)]
- as required or permitted by law (see examples under "report" in the Glossary).

For more information about disclosure, refer to sections 38-50 in PHIPA, the *Health Protection and Promotion Act, 1990* (HPPA) or the IPC.

Accountabilities

To uphold the principle of disclosure, nurses must:

- take reasonable steps to provide care interactions in a private setting to maintain confidentiality
- obtain express consent from the client or substitute decision-maker before disclosing client information outside the health care team
- ensure confidentiality during disclosure of personal health information, whether verbally, in hard copy or electronic form (for example, email or instant messaging)
- assess whether disclosure may result in any harm to the client, and consult the health care team when there are concerns about potential harm from sharing information

- advise the client of any duty to report information to another agency or facility
- report information as required by law (for example, *Child, Youth and Family Services Act, 2017*, HPPA, RHPA)
- offer the client the opportunity to report information themselves when appropriate (for example, informing a partner about possible sexually transmitted and blood-borne infections)
- notify the appropriate authority if the client does not report information themselves
- verify that anyone requesting information has the legal authority to access it (for example, police officers who request with a court order)
- seek guidance from the designated contact person required under PHIPA before releasing information
- report any suspected or known confidentiality breaches and follow employer/organizational protocol for stolen, lost or improperly accessed personal health information.

Partners in Safety

In Ontario's health care system, employers and organizations that are HICs — as well as nurses who are self-employed HICs — have primary responsibility for protecting the confidentiality and privacy of personal health information. HICs are accountable for the personal health information in their custody or control, and for the actions of their agents (including nurses and third parties) who access, collect, use or disclose that information on their behalf. HICs must provide notice to clients about information practices and ensure that clients are aware of their personal health information privacy rights.

Employers, as HICs, support agents in meeting their legal and professional obligations by establishing privacy-protective work environments, providing clear policies and procedures, delivering education and training, and implementing secure administrative, physical and electronic safeguards. These systems enable nurses to comply with legislation and CNO practice standards.

All employers have a duty to the public to align confidentiality and privacy practices with current legislation so that they support client safety and public trust.

HICs are also responsible for safeguarding the privacy and confidentiality of clients if their organization chooses to use technologies such as AI. Having a strong governance and accountability framework established before using an AI system is critical to upholding privacy by design principles and ensuring ongoing compliance with PHIPA (IPC, 2026). These policies, procedures and practices should clearly set out the accountabilities of the HIC, their agents, (which can include nurses) and others who act on their behalf, including third-party service providers (IPC, 2026).

All partners in safety, including HICs, employers and nurses, share the responsibility for creating environments that support quality practice. Nurses should advocate for policies and procedures that protect confidentiality when none exist.

Nurses must report any suspected or known privacy breaches and follow employer/organizational procedures. HICs are responsible for notifying individuals (and if legally required, the IPC) when health information is stolen or lost, or if it is used or disclosed without the necessary authority (PHIPA, s 12). HICs are also responsible for submitting a privacy breach annual report, which must include incidents that did not meet the threshold for individual reporting to the IPC.

Glossary

Agent: People who are authorized to act for, or on behalf of, a Health Information Custodian (HIC), as per the *Personal Health Information Protection Act, 2004* (PHIPA, s 2). In general, nurses who are employees or volunteers, or contracted or credentialed by a health care organization, such as a clinic, laboratory, home and community care providers, hospital or long-term care facility, are considered "agents" of a HIC. (Virtual Care, 2026).

Artificial intelligence (AI): Encompasses a broad spectrum of technologies aimed at mimicking cognitive functions associated with human intelligence (Virtual Care, 2026).

Collection: In relation to personal health information, means to gather, acquire, receive or obtain the information by any means from any source [PHIPA, ss 4(2)].

Client: An individual, family, group, community or population receiving nursing care, including, but not limited to, "patients" or "residents" (Code of Conduct, 2026).

Consent directive: A directive that withholds or withdraws, in whole or in part, the individual's consent to the collection, use and disclosure of his or her personal health information by means of the electronic health record by a Health Information Custodian for the purposes of providing or assisting in the provision of health care to the individual [PHIPA, ss 1 (16)].

Data minimization: Refers to the collection, use and disclosure of only the personal information reasonably necessary to meet the purposes of the collection, use or disclosure, as the case may be [PHIPA, ss 30(2)].

Disclosure: Means to make the information available or to release it to another health information custodian or to another person, in the custody or under the control of a Health Information Custodian or a person. Does not include to use the information (PHIPA, s 2).

Express consent: Verbal or written approval from an individual to a Health Information Custodian to collect, use or disclose the individual's personal health information for a specific purpose (IPC, n.d.-c).

Health care team: Members of the intraprofessional and/or interprofessional team and/or community supporting client care. This also includes students, new learners and Indigenous and traditional healers (Code of Conduct, 2026).

Health information custodian (HIC): A person or organization listed in the *Personal Health Information Protection Act, 2004* (PHIPA) that, as a result of their power or duties or work set out in PHIPA, has custody or control of personal health information (IPC, September 2015). HICs are responsible for practices and policies that ensure the confidentiality and security of personal health information and complying with PHIPA.

Identifying information: Information that identifies an individual or for which it is reasonably foreseeable that it could be used, either alone or with other information, to identify an individual (PHIPA, s 4(2)).

Indirect collection: the collection of personal health information from someone other than the client, with or without consent.

Informed consent: As described under the *Health Care Consent Act, 1996*, a person's consent is informed if the person receives information about a treatment that a reasonable person in the same circumstances would

require to make a decision and if the person receives responses to their requests for additional information about the treatment.

The information must include the treatment's nature, expected benefits, material risks and side effects; alternative courses of action; and likely consequences of not having the treatment (Code of Conduct, 2026).

Individual: In relation to personal health information in the *Personal Health Information Protection Act, 2004*, means the individual, whether living or deceased, with respect to whom the information was or is being collected or created (PHIPA, s 2).

Information privacy: The client's right to control how their personal health information is collected, used and disclosed.

Information and Privacy Commissioner of Ontario (IPC): Provides oversight of Ontario's laws that establish rules for the way institutions may collect, use, and disclose your personal information (IPC, n.d.-a).

Lockbox: Term commonly used to describe the rights of individuals to withhold or withdraw their consent to the collection, use or disclosure of their personal health information for health care purposes (IPC, September 2015).

Personal health information: Identifying information about clients in oral or recorded form as described in the *Personal Health Information Protection Act, 2004*, ss 4(1).

Personal information: Any information in oral or recorded form that could be used either on its own, or in combination with other available information, to identify an individual (Government of Ontario, 2024).

Professional misconduct: An act or omission that contravenes nurses' legislated obligations and/or the standards of practice and ethics of the profession. Professional misconduct is defined in section 51(1) of the Health Professions Procedural Code, which is Schedule 2 to the *Regulated Health Professions Act, 1991*, and further described in the Professional Misconduct regulation (O. Reg. 799/93) under the *Nursing Act, 1991*.

Quality of care information: Information defined in the *Quality of Care Information Protection Act, 2016* that:

(a) is collected or prepared for a quality of care committee for the sole or primary purpose of assisting the committee in carrying out its quality of care functions

(b) relates to the discussions and deliberations of a quality of care committee in carrying out its quality of care functions

(c) relates solely or primarily to any activity that a quality of care committee carries on as part of its quality of care functions, including information contained in records that a quality of care committee creates or maintains related to its quality of care functions [*Quality of Care Information Protection Act*, ss 2(2)].

Quality of care information does not include any of the following:

1. Information contained in a patient record.
2. Information contained in a record that is required by law to be created or to be maintained.
3. Information relating to a patient in respect of a critical incident that describes,
    i. facts of what occurred with respect to the incident,
    ii. what the quality of care committee or health facility has identified, if anything, as the cause or causes of the incident,
    iii. the consequences of the critical incident for the patient, as they become known,
    iv. the actions taken and recommended to be taken to address the consequences of the critical incident for the patient, including any health care or treatment that is advisable, or

v. the systemic steps, if any, that a health facility is taking or has taken in order to avoid or reduce the risk of further similar incidents.

4. Information that consists of facts contained in a record of an incident involving the provision of health care to a patient.

5. Information that a regulation specifies is not quality of care information and that a quality of care committee collects or prepares after the day on which that regulation comes into force [*Quality of Care Information Protection Act*, ss 2(3)].

Record: Information in any form or medium, including written, printed, photographic or electronic form or otherwise, but does not include a computer program or other mechanism that can produce a record (PHIPA, s 2).

Report: The legal and organizational requirement to disclose safety issues related to health care professionals' individual practice, or issues impacting practice settings (Code of Conduct, 2026). Examples of legal reporting requirements include:

- Reporting to proper authorities any health care team member whose actions or behaviours toward clients are unsafe or unprofessional according to applicable legislation, including, but not limited to, the *Fixing Long-Term Care Homes Act, 2021*, *Child, Youth and Family Services Act, 2017*, *Public Hospitals Act*, and the *Retirement Homes Act, 2010.*
- Reporting a regulated health professional's sexual abuse of a client to the Registrar of the proper regulatory college according to the *Regulated Health Professions Act, 1991*.
- *Health Protection and Promotion Act* permits a practitioner to disclose personal health information related to reporting of a communicable disease, a disease of public health significance, a virulent disease or a reportable event following the administration of an immunization agent without obtaining consent in certain circumstances.

Security: The processes and tools that ensure confidentiality of information.

Self-employed: Nurses who are self-employed own their own economic enterprise or have a financial investment in the enterprise for the purposes of offering nursing services (Independent Practice, 2025).

Social media: Online communication tools (websites and applications) used for interaction, content sharing and collaboration. Types of social media include blogs or microblogs (personal, professional, or anonymous), discussion forums, message boards, social networking sites and content-sharing websites (Code of Conduct, 2026).

Substitute decision-maker: Person, identified by the *Health Care Consent Act, 1996*, who makes a treatment decision for someone who cannot make their own decision. See CNO's *Consent* guideline for more information (Code of Conduct, 2026).

Unauthorized access: The collection, use or disclosure of personal health information without the consent of clients for purposes that are not permitted or required by PHIPA (IPC, n.d.-d).

Use: To view, handle or otherwise deal with personal health information in the custody or under the control of a Health Information Custodian or a person. Does not include the disclosure of information (PHIPA, s 2).

Virtual care: The delivery, management and coordination of health services using electronic information and digital telecommunication technologies to provide client-centred care (Virtual Care, 2026).

References

Canadian Nurses Protective Society. (2021). *InfoLAW: Privacy and Electronic Medical Records.* https://cnps.ca/article/privacy-and-electronic-medical-records/

Child, Youth and Family Services Act, 2017, SO. 2017, c 14, Sched 1. https://www.ontario.ca/laws/statute/17c14

College of Nurses of Ontario. (n.d.) *Artificial intelligence in nursing practice.* https://cno.org/standards-learning/educational-tools/artificial-intelligence-in-nursing-practice

College of Nurses of Ontario. (2026). *Code of Conduct.* https://www.cno.org/Assets/CNO/Documents/Standard-and-Learning/Practice-Standards/49040_code-of-conduct.pdf

College of Nurses of Ontario. (2026). *Virtual Care.* https://www.cno.org/Assets/CNO/Documents/Standard-and-Learning/Practice-Standards/practice-guideline-virtual-care-en.pdf

College of Nurses of Ontario. (2025). *Independent Practice.* https://cno.org/Assets/CNO/Documents/Standard-and-Learning/Practice-Standards/41011_fsindepprac.pdf

Connecting Care Act, 2019, SO 2019, c 5, Sched 1. *https://www.ontario.ca/laws/statute/19c05*

Fixing Long-Term Care Act, 2021, SO 2021, c 39, Sched 1. https://www.ontario.ca/laws/statute/21f39

Freedom of Information and Protection of Privacy Act, RSO 1990, c.F.31. https://www.ontario.ca/laws/statute/90f31

Government of Ontario. (2024). *Guidance on information sharing.* https://www.ontario.ca/page/guidance-information-sharing#section-7

Health Care Consent Act, 1996, SO 1996, c 2, Sched A. https://www.ontario.ca/laws/statute/96h02

Health Protection and Promotion Act, RSO 1990, c H.7. https://www.ontario.ca/laws/statute/90h07

Information and Privacy Commissioner of Ontario. (n.d.-a). *About Us.* https://www.ipc.on.ca/en/about-us

Information and Privacy Commissioner of Ontario. (n.d.-b). *Accessing or correcting your personal health information.* https://www.ipc.on.ca/en/health-individuals/accessing-or-correcting-your-personal-health-information

Information and Privacy Commissioner of Ontario. (n.d.-c). *Consent and your personal health information.* https://www.ipc.on.ca/en/health-individuals/consent-and-your-personal-health-information

Information and Privacy Commissioner of Ontario. (n.d.-d) *Unauthorized access.* https://www.ipc.on.ca/en/health-organizations/unauthorized-access

Information and Privacy Commissioner of Ontario. (2015, August). *Circle of Care: Sharing Personal Health Information for Health-Care Purposes.* https://www.ipc.on.ca/en/resources-and-decisions/circle-care-sharing-personal-health-information-health-care-purposes

Information and Privacy Commissioner of Ontario. (2015, September). *Frequently Asked Questions: Personal Health Information Protection Act*. https://www.ipc.on.ca/sites/default/files/legacy/2015/11/phipa-faq.pdf

Information and Privacy Commissioner of Ontario. (2026, January). *AI Scribes: Key Considerations for the Health Sector*. https://www.ipc.on.ca/en/resources/ai-scribes-key-considerations-health-sector

Nursing Act, 1991, SO 1991, c 32. https://www.ontario.ca/laws/statute/91n32

Personal Health Information Protection Act, *2004*, SO 2004, c 3. Sched A. https://www.ontario.ca/laws/statute/04p03

Public Hospitals Act, RSO 1990, c P.40. https://www.ontario.ca/laws/statute/90p40

Regulated Health Professions Act, 1991, SO 1991, c 18. https://www.ontario.ca/laws/statute/91r18

Retirement Homes Act, 2010, SO 2010, c 11. https://www.ontario.ca/laws/statute/10r11

Quality of Care Information Protection Act, 2016, SO 2016, c 6, Sched 2. https://www.ontario.ca/laws/statute/16q06

Substitute Decisions Act, 1992, SO 1992, c 30. https://www.ontario.ca/laws/statute/92s30

For more information

To learn more, contact the College of Nurses of Ontario at:
Telephone: 416 928-0900
Toll-free in Canada: 1 800 387-5526
email: cno@cnomail.org
Fax: 416 928-6507
Website: www.cno.org

COLLEGE OF NURSES OF ONTARIO
ORDRE DES INFIRMIÈRES ET INFIRMIERS DE L'ONTARIO

101 Davenport Rd.
Toronto, ON
M5R 3P1
www.cno.org

Tel.: 416 928-0900
Toll-free in Canada: 1 800 387-5526
Fax: 416 928-6507
Email: cno@cnomail.org