College of Registered Nurses of Manitoba

Maintaining Privacy and Confidentiality

Purpose

The public expects ethical and competent service from all registered nurses (RNs), RN(AP)s, RN(NP)s and from the whole health-care system. RNs are responsible to act according to the ethical responsibilities in the *Code of Ethical Conduct*. Privacy and confidentiality are ethical values that support the clients' autonomy and dignity. Trustworthiness develops when clients' privacy and confidentiality are respected and protected. Trust is an essential factor for clients to work effectively with care providers.

RNs hold a fundamental obligation regarding privacy and confidentiality of personal health information. Privacy is embedded in the Practice Expectations for RNs and the *Code of Ethical Conduct*. RNs must apply the knowledge, skills, and judgment required to meet their practice expectations. RNs have an ethical responsibility to respect the interests of clients via the lawful collection, use, access, and disclosure of personal information. They are expected to value privacy, confidentiality and safeguard personal health information obtained in the context of a professional relationship.

The purpose of this document is to outline reasons for privacy and confidentiality and to offer information about application of the *Code of Ethical Conduct* to safeguard privacy and confidentiality in some common personal health information breaches

Background

Across Canada, privacy is a right. The *Canadian Charter of Rights and Freedoms*, the *Privacy Act*, and Manitoba's *Freedom of Information and Protection of Privacy Act*, provide legislation for protection of personal information that is held by private institutions and governments.

Manitoba's *Personal Health Information Act* (PHIA) sets out rules for both the protection of and access to personal health information. Personal health information is recorded information that can be connected to a specific person, including data of one's health, history, health care provided and received. It also includes information such as name, birthdate, gender and address if that information was collected during health care service or used to administer fees for care. The government of Manitoba contains more information about this legislation in frequently asked questions (gov.mb.ca). With PHIA, the public expects:

- Confidentiality of personal health information,
- Secure collection, storage and maintenance of personal health information,
- Information as to why one's own personal health information is being collected,
- A process to access one's own personal health information, and
- A right to request a correction to one's personal health information.

Breaches to privacy and confidentiality may be categorized as either improper access to personal health information, inappropriate disclosure of personal health information and/or a failure to safeguard personal health information.

Improper Access to Personal Health Information

Example: For Another Person

RNs may be asked to look up personal health information for someone else, such as a friend or family member. The RN may be part of the family or friend's natural support system, which is a role outside of their workplace. While electronic health records afford easy access to large numbers of health records, this does not mean that a RN may use workplace credentials to look up someone else's health information through unauthorized access. The same goes for non-electronic or paper-based health records, it is still inappropriate to look up personal health information for someone else when the RN is not part of their health care team. There is a risk that the RN may not have the full context of the person's health care situation and misinterpret the results; or the person may not follow-up with their health care provider for further diagnostic testing, care planning or treatment, which in turn could lead to poorer health outcomes.

Even if a family member or a friend has given permission to the RN to look up their personal health information or provide test results to family or a friend before they return to their healthcare provider, it is unauthorized access. The *Code of Ethical Conduct* outlines the ethical responsibility to not abuse information access by accessing health-care records for a purpose that is not consistent with their professional obligation. As per the *Code of Ethical Conduct*, RNs have a responsibility to keep appropriate professional boundaries; using workplace privileges for personal reasons is crossing a professional boundary.

An appropriate response to any request to use workplace credentials for unauthorized access is to refuse and redirect the person to their health care provider. Providing information about returning to their health care provider and/or making a request to the trustee for the information can also be helpful. The individual or anyone with written permission to act on behalf of the individual may request access to the individual's personal health information directly to the health care provider or the trustee of the health information. More information about the process to access personal health information can be found through the trustee or Manitoba Health Frequently Asked Questions | PHIA | Manitoba Health | (gov.mb.ca).

Example: When the RN is Not Part of the Client's Health Care Team

RNs may work, collaborate or consult with a health-care team however, the RN may not be involved in caring for every client. Hospitals, personal care homes, clinics, public health, and health/nursing agencies are just a few examples. On a realistic, need-to-know basis, personal health information may be shared within the client's healthcare team for the purpose of either consulting on or providing care. Such care includes direct clinical care and non-clinical health-related work such as assessment, diagnosis, treatment, monitoring, surveillance, health communications, coordination, and management. This is in-keeping with the *Code of Ethical Conduct* responsibility to collect, use and disclose health information on a need-to-know basis with the highest degree of anonymity possible in the circumstances and in accordance with privacy laws.

On the other hand, when the RN is not involved in or consulted on the client's health and care, the RN does not have a reasonable need to access or learn personal health information about that client. For example, checking out a client's health record before the RN is consulted, or referred for care, just in case the client may be assigned to the RN in the future would be considered snooping. The same applies when the RN is no longer providing care as there is no reasonable need-to-know (e.g. a client is transferred away from your unit or service and not scheduled to return). Interest in learning how the client fared post-discharge or other curiosity does not excuse snooping.

Example: One's Own Personal Health Information

When personal health information is contained in a health care record, it belongs to the trustee of this information. Anyone, including RNs, may only access their own health records if they follow a process required by PHIA and make a request directly to the trustee who maintains the health care records. For example, if the personal health information was collected at a primary care clinic, the request should go to the trustee of the clinic.

Even when the RN has workplace access at the location where their own personal health information is stored, this does not include permission to skip the process to ask the trustee. Use of workplace credentials to view one's own personal health information goes beyond any privileges granted by the trustee. Any reason, whether it be the speed or ease of direct access is not valid and constitutes an abuse of the RN's workplace access. The *Code of Ethical Conduct* provides the ethical responsibility to not abuse information access by accessing health-care records for a purpose that is not consistent with one's professional obligation.

Disclosing Personal Health Information

Example: Outside a Client's Circle of Care

It is helpful to distinguish between use of a client's personal health information for the provision of health care from the disclosure (either authorized or unauthorized disclosure) of a client's personal health information to someone else.

Use of personal health information occurs when health care providers within the trustee's organization need to see and use personal health information to provide care. Authorized disclosure occurs when personal health information is provided to people outside the organization with the client's consent or as permitted by PHIA. For a complete list of authorized disclosures without consent, see sections 21 through 25 of PHIA. C.C.S.M. c. P33.5 (gov.mb.ca). Examples (not all inclusive) of authorized disclosure without consent include providing information to:

- A person who is, will be, or has provided health care to the client, but only enough information to provide health care to the client (unless the client has instructed no disclosure of personal health information).
- An immediate family member, or to anyone who the client has a close personal relationship with, if the disclosure is about health care currently provided, is made according to professional practice, and the trustee reasonably believes that disclosure is acceptable to the client.
- Any person, to prevent or lessen a risk of harm to a minor's health/safety.
- Any person, to prevent or lessen a risk of serious harm to the health/safety of any individual, public health or public safety.
- Any person, as authorized or required by an enactment of Manitoba or Canada (e.g. Child and Family Services Act (Indigenous Jurisdiction and Related Amendments), Mental Health Act clause 36).

Examples of unauthorized disclosure of personal health information include:

- Providing information to anyone outside the client's circle of care (e.g. gossiping or telling a story),
- Sharing information in public areas where people not in the client's circle of care may overhear.

The *Code of Ethical Conduct* asserts the responsibility to:

- Take reasonable steps to prevent people from overhearing confidential information, and
- Disclose only the amount of information necessary and inform only the people necessary.

Jeopardizing Safeguards for Personal Health Information

Example: Leaving or Forgetting Information or Passwords in an Accessible Area

The chance to make a mistake and leave personal health information in places accessible to other people abound. Walking away from an electronic medical record without logging out, even just for a moment, creates the possibility that another person may see personal health information on the screen even when this was not the intention. Not locking a screen when stepping away from an electronic medical record also creates the risk that someone can easily access a large amount of personal health information using your credentials. Even placing passwords under the keyboard (or another typical spot) or sharing passwords are opportunities for another person to gain unauthorized access to personal health information.

The same unauthorized access can occur leaving a paper-based client record or client notes in a publicly visible area. Consider an open chart at the front desk where visitors can either inadvertently or deliberately read the open record, or "nursing notes" left behind at the client's bedside or any public area, as examples.

While these examples may appear obvious and easy to avoid, the reality is this continues to occur. Locking a computer screen before stepping away, closing, and putting away a chart, checking to be sure any notes are not left behind, and shredding confidential information are just a few ways to safeguard personal health information. These actions are part of the RN's ethical responsibility to protect and preserve the privacy of persons receiving care, including security safeguards in information technology. It is an essential way for RNs to demonstrate trustworthiness.

Definitions

Disclosure: revealing personal health information outside the trustee organization to other trustees, to the individual's friends and family or to other individuals. Both use and disclosure involve revealing the information to someone. This may be done by permitting others to read it, sending it to them by mail, fax, e-mail or by revealing the information orally. Disclosure may be either authorized such as with a client's consent or as permitted by PHIA, or unauthorized such as through inattention or inappropriate action.

Personal Health Information: recorded information about an identifiable individual that relates to the individual's health, or health care history, including genetic information about the individual, the provision of health care to the individual, or payment for health care provided to the individual. It includes the PHIN and any other identifying number, or symbol assigned to an individual, and any identifying information about the individual that is collected during, and is incidental to, the provision of health care or payment for health care.

Trustee: a health professional, health care facility, public body, or health services agency that collects or maintains personal health information. Examples of trustees are health professionals such as self-employed RNs, hospitals, personal care homes, community health centres, medical clinics, ambulance services, laboratories, regional health authorities, and public bodies such as government departments, crown corporations and school divisions.

Use: what is done with the personal health information within the trustee organization such as for the provision of client care.

References

Canadian Nurses Protective Society (2021). InfoLAW: Confidentiality of Health Information (cnps.ca).

CRNM (2025) Code of Ethical Conduct www.crnm.mb.ca.

CRNM (2022). *Practice Direction: Practice Expectations for RNs*. www.crnm.mb.ca.

Government of Canada (1982). The Canadian Charter of Rights and Freedoms (justice.gc.ca).

Government of Canada (1985). The Privacy Act. (R.S.C., 1985, c. P-21).

Government of Manitoba (1997). The Personal Health Information Act (PHIA) (gov.mb.ca).

Government of Manitoba (2023). *Child and Family Services Act (Indigenous Jurisdiction and Related Amendments)*. https://web2.gov.mb.ca/laws/statutes/2023/c02623.php?lang=en#48.

Government of Manitoba (2024). *Frequently Asked Questions About PHIA*. Manitoba Health (gov.mb.ca)

Government of Manitoba (n.d.). *Freedom of Information and Privacy Act*. Freedom of Information and Protection of Privacy Act (gov.mb.ca).

Province of Manitoba (n.d.). *Manitoba's Mental Health Act*. Province of Manitoba | Mental Health and Addictions (gov.mb.ca)

Shen, N. et el. (2019). Understanding the patient privacy perspective on health information exchange: A systematic review. *International Journal of Medical Informatics, 125, 1-12*.

Revised: 03/24
Published: 03/2024

For more information please contact one of our quality practice consultants at

204-774-3477

800-665-2027 (Manitoba toll-free)

Our publications are available on our website at crnm.mb.ca