Need-to-Know Instead of Circle of Care

Office of the Information and Privacy Commissioner for Nova Scotia
January 24, 2024

Notice to Users

This document is intended to provide general information only. It is not intended nor can it be relied upon as legal advice. As an independent agency mandated to oversee compliance with *FOIPOP*, *MGA* and *PHIA* the Office of the Information and Privacy Commissioner for Nova Scotia cannot approve in advance any proposal from a public body, municipal body or health custodian. We must maintain our ability to investigate any complaints and to provide recommendations in response to these complaints. The contents of this document do not fetter or bind this office with respect to any matter, including any complaint investigation or other matter respecting which the Commissioner (Review Officer) will keep an open mind. It remains the responsibility of each public body, municipal body and health custodian to ensure that they comply with their responsibilities under the relevant legislation. Visit us at: https://oipc.novascotia.ca.

WHAT IS THE CIRCLE OF CARE?

The term "circle of care" does not appear in Nova Scotia's *Personal Health Information Act (PHIA)*. In health care, it is used to describe the team of health-care providers involved in a patient's care and their ability to access and share information using implied consent. However, as the following Saskatchewan case illustrates, applying this concept in a privacy context can cause confusion and lead providers to believe they are authorized to access patient information when, under privacy law, they are not. Rather, the concept of "circle of care" should be replaced with "need-to-know."

CIRCLE OF CARE CONCEPT vs. NEED-TO-KNOW PRINCIPLE

In *Stebner v. CBC,*[1] a physician sought to block Saskatchewan's Information and Privacy Commissioner (IPC) from publishing a report that found she had breached the privacy of three Humboldt Bronco hockey players after the 2018 bus crash. The physician argued that she was part of the circle of care. She believed she had treated two of the individuals in hospital before the crash and had viewed their information as she anticipated she might possibly be called upon to care for one of them when she returned to the hospital in two weeks time. The judge rejected the concept of circle of care and affirmed the correct test was whether she had a need to know the information.

The judge quoted the IPC's comments to highlight the weaknesses of the circle of care as a concept when it comes to privacy law. The concept puts the focus on the provider and whether they are a "member of the club" and implies "a static kind of entitlement to information" instead of focusing on the patient and the uniqueness of the care being sought. This is problematic because the circle of care should change based on the treatment being provided. An individual who is treated in an emergency department for a broken arm one day and then visits a pharmacy for birth control the next month has a different circle of care for each visit. Under modern health privacy law, the focus should be on the patient's health needs in a particular encounter and information should only be accessed on a need-to-know basis.

NEED-TO-KNOW PRINCIPLE

The need-to-know principle holds that providers can only access and use the personal health information they need to know to carry out their responsibilities for a patient encounter. It is incorporated into section 25 of Nova Scotia's *PHIA.* To avoid confusion and non-compliance with *PHIA*, custodians must embed the need-to-know principle into their practice. The following measures can help:

- Document the tasks and information needs of each role in your practice. Discuss with your employees.
- Ensure confidentiality agreements and privacy training incorporate the need-to-know principle, not the circle of care. Review them with employees annually. Include practical

[1] *Stebner v Canadian Broadcasting Corporation*, 2019 SKQB 91 (CanLII)

examples of what staff do and do not need to know in their role. Highlight consequences for non-compliance.
- Use technical controls to restrict staff electronic medical record (EMR) access to what they need to know.
- Regularly monitor EMR audit logs for unauthorized access. Make staff aware access is audited. Investigate incidents thoroughly and ensure consequences are consistently enforced. Report unauthorized accesses to affected individuals.

CONCLUSION

By fostering a culture of privacy based on the need-to-know principle, custodians can protect their patients' information from unauthorized access, comply with *PHIA* and maintain patient trust.

QUESTIONS?

This guidance was prepared by the Office of the Information and Privacy Commissioner for Nova Scotia. We encourage organizations to contact us with any questions about this document. Organizations can also consult with our office for free by completing and submitting a Consultation Request Form:

- Consultation Request Guidelines
- Consultation Request Form

Phone: 902-424-4684
Toll Free (NS): 1-866-243-1564
TDD/TTY: 1-800-855-0511
Fax: 902-424-8303
Email: oipcns@novascotia.ca