Information and Privacy Commissioner,
Ontario, Canada

Commissaire à l'information et à la protection de la vie privée,
Ontario, Canada

PHIPA DECISION 290

Complaint HR24-00118

Maamwesying North Shore Community Health Services

July 17, 2025

Summary: Maamwesying North Shore Community Health Services (the custodian) reported a privacy breach to the Office of the Information and Privacy Commissioner of Ontario (the IPC) under the *Personal Health Information Protection Act, 2004* (the *Act*). At the time of the breach, the custodian, in partnership with an Indigenous community, provided health care services at the community's local health centre.

In January 2024, the custodian received lockbox requests from a large number of the community's patients seeking to restrict chart access by a registered nurse, who was both an agent of the custodian and an employee of that community. The custodian investigated and determined that the nurse viewed without authorization electronic charts of patients to whom she did not provide care. Later, the custodian also reported that the nurse disclosed without authorization patients' personal health information in an offsite meeting between the nurse and other community staff.

Following its investigation into the matter, the custodian found that the nurse viewed patients' health records without authorization. The custodian removed her access to all electronic medical records and relieved her of her duties. To remediate the breaches, the custodian adopted a new policy to improve training and onboarding for new agents, implemented safeguards for the electronic medical records system and completed initiatives to improve privacy awareness for partner communities.

In this case, the IPC investigator finds that, at the time of the breaches, the custodian did not have in place reasonable measures to protect personal health information from unauthorized use and disclosure, as required by section 12 of the *Act.* Nevertheless, based on the remedial steps taken, the investigator finds the custodian responded adequately to the breaches and that further review under Part VI of the *Act* is not warranted.

Statutes Considered: *Personal Health Information Protection Act, 2004, S.O. 2004, c. 3,* sections 2, 10(1), 10(2), 12(1) and 12(2)

Decisions Considered: PHIPA Decisions 110, 155 and 260

BACKGROUND:

[1] On February 23, 2024, Maamwesying North Shore Community Health Services (the custodian) reported a privacy breach to the Office of the Information and Privacy Commissioner of Ontario (the IPC) under the *Personal Health Information Protection Act, 2004* (the *Act* or *PHIPA*). The breach related to unauthorized access of personal health information by a registered nurse.

[2] During the early resolution stage of the IPC's *PHIPA* complaint process, the custodian provided information related to the unauthorized access and the steps they took in response to the breach. After review of the information, the file was moved to the investigation stage, and I was assigned as the investigator. During my investigation, I requested and received written representations from the custodian.

[3] The custodian provides primary care, home and community support services and mental health and addiction services to Indigenous people and members of different Indigenous communities in their respective health centres. Through partnerships with the custodian, these communities provide their employees, including health care practitioners, to work as agents for the custodian (called community agents). The custodian maintains an electronic medical records system (the EMR), which the community agents access remotely to perform their duties.

[4] The breaches in this case involved one community agent of the custodian, a registered nurse who was an employee of one of the custodian's partner Indigenous communities. At the time of the breaches, the nurse was working as agent for the custodian in the role of a Community Health Nurse.

[5] In January 2024, a Client Care Coordinator from the community reported to the custodian that they received a large volume of lockbox requests from its members.[1] These requests sought to restrict patient chart access by the nurse.

[6] In light of the large number of lockbox requests received and as a precautionary measure, the custodian removed all paper-based patient charts from the community's health centre. The custodian proceeded to implement the lockbox requests and inform the patients. Between January and March 2024, the custodian processed a total of 27

[1] Under the *Act,* individuals may withhold or withdraw their consent to the collection, use or disclosure of their PHI by health information custodians for the purposes of providing or assisting in providing health care; *see* the IPC's guidance on lockbox requests available online: <https://www.ipc.on.ca/en/resources-and-decisions/fact-sheet-08-lock-box-fact-sheet>.

lockbox requests in relation to the nurse.

[7] The custodian informed the nurse about the limitations imposed by the lockboxes. It was determined that the nurse had not completed privacy training or signed a confidentiality agreement as part of her onboarding process, and these requirements were fulfilled in late January 2024.

[8] The custodian also launched an internal investigation pursuant to their privacy breach protocol and other internal policies. As part of their investigation, they obtained audit results on the nurse's access to patient records in the EMR. It was eventually confirmed that between October 23, 2023 and January 24, 2024, the nurse viewed without authorization electronic charts of 34 patients. These patients had not received health care from the nurse and were considered outside her circle of care. The investigation also determined that no physical records were inappropriately accessed by the nurse.

[9] The accessed patient records in the EMR contained various types of personal health information, such as:

- Name, address, phone number, and email address;
- Health card number;
- Date of birth;
- Next visit date;
- Family history;
- Medical conditions;
- Immunization record;
- Referral forms;
- Encounter notes;
- Progress notes;
- Diagnostic imaging requests;
- Lab requisitions; and
- Smoking status.

[10] Following the investigation which included an interview with the nurse, the custodian terminated her EMR access on February 22, 2024. The custodian relieved the

nurse of her duties by way of notification to the Indigenous community's leadership in March 2024. The custodian also reported the matter to the College of Nurses of Ontario.

[11] In March 2024, the custodian notified the affected patients, except two individuals whose contact information could not be located. Further to the IPC's recommendation, the custodian placed a note in their charts so that if contact is re-established in the future, the patients would be informed about the breach.

[12] The custodian advised that due to the privacy incident and other administrative concerns, they no longer maintain partnership with the Indigenous community that employed the nurse. In April 2024, the custodian relocated their care services from the community's local health centre to an alternative site so that continuity of care would be maintained for the community's members.

[13] During the IPC's investigation, the custodian also reported that they obtained new information about potential unauthorized disclosure of personal health information. The custodian had known previously that on December 18, 2023, the nurse's laptop was removed without authorization from the community health centre where the custodian provided care services. The custodian received additional information from a staff member who was present at the community's band office that day. According to the information received, the nurse's laptop was taken to a conference room in the band office, where she met with the assistant to the community's Chief, a council member and an employee of the community between 9 am and noon.

[14] Since this information raised concerns of potential unauthorized disclosure of personal health information, the custodian launched a further investigation. A review of the EMR log revealed that between 9 am and noon of December 18, 2023, the nurse viewed charts associated with seven patients, the same viewings that were previously reported to the IPC as unauthorized access and for which the patients were notified. The custodian also observed that on the same day at 11:12 am, the nurse emailed the custodian's Data Management Specialist to request a copy of the custodian's active client list, which she received later. Based on their investigation which included information provided by the affected patients, the custodian concluded that during the course of this off-site meeting, the nurse disclosed without authorization personal health information contained in the seven patients' electronic charts.

[15] Following discussions with the IPC, the custodian directly notified in April 2025 the seven patients. The notice explained that as part of their investigation, the custodian asked the nurse to respond to the allegation of disclosure and to explain the laptop removal from the health centre and her access to patients' health records. The notice stated that the nurse denied that the incident occurred, and that the custodian concluded that patients' information was shared with the band office members without authorization.

PRELIMINARY ISSUES:

[16] There is no dispute, and I find, that the custodian is a "health information custodian" as defined under section 3(1) of the *Act* and that the nurse was the custodian's agent as defined under section 2 of the *Act.*

[17] Furthermore, it is not in dispute that the nurse accessed and disclosed without authorization records of "personal health information" within the custody or control of the custodian. Accordingly, I find that there was an unauthorized use and disclosure of personal health information [as defined under section 4(1)] contrary to section 29 of the *Act*.

ISSUE:

[18] In this decision, I address whether the custodian took reasonable steps to protect personal health information.

RESULTS OF THE INVESTIGATION:

Did the custodian take reasonable steps to protect personal health information?

[19] Sections 12(1) and 12(2) of the *Act* state:

> 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.
>
> …
>
> (2) Subject to subsection (4) and to the exceptions and additional requirements, if any, that are prescribed, if personal health information about an individual that is in the custody or control of a health information custodian is stolen or lost or if it is used or disclosed without authority, the health information custodian shall,
>
> (a) notify the individual at the first reasonable opportunity of the theft or loss or of the unauthorized use or disclosure; and
>
> (b) include in the notice a statement that the individual is entitled to make a complaint to the Commissioner under Part VI.

[20] The IPC has recognized that health information custodians must take "reasonable" steps to protect personal health information (PHI) in their custody or control from a privacy breach, such as unauthorized use or disclosure of PHI.[2] In addition, custodians have a duty to respond promptly and adequately to a breach, taking appropriate steps to contain, investigate and remediate the breach, and to notify affected individuals.[3] The IPC has recognized that the standard in section 12(1) is reasonableness; it does not require perfection and the section does not provide a detailed prescription for what is reasonable.[4]

[21] A related obligation is the duty under sections 10(1) and 10(2) for health information custodians to have in place and follow information practices which comply with the requirements of the *Act*. [5]As defined under the *Act,* information practices include administrative, technical and physical safeguards and practices with respect to personal health information.[6]

[22] Based on the information received, I am generally satisfied with the containment steps taken after the custodian was notified of the lockbox requests submitted regarding the nurse.

[23] The IPC received details from the custodian related to their investigation, which began promptly after containment. An audit was initiated to review the nurse's EMR access log since her onboarding. The custodian also conducted interviews with the nurse and other staff members. In particular, the custodian interviewed the data management specialist and reviewed the relevant documentation to evaluate the responses from the nurse, to ascertain how she established her access to the EMR and whether she underwent the appropriate onboarding process. I am satisfied overall that the custodian's investigation into the circumstances of the breaches was adequate.

[24] The breaches in this case raised concerns related to policies and practices that specifically address the custodian's management of community agents, EMR access, training, and confidentiality agreements. Furthermore, I considered the information submitted related to the custodian's audit capability. In the discussion below, I focus on these concerns and the remedial steps the custodian took in response to the breaches.

Management of community agents

Onboarding process

[25] I asked the custodian to clarify how they establish and maintain their relationship

---

[2] PHIPA Decision 260 at para 27.
[3] *S*ee Information and Privacy Commissioner of Ontario (October 2018), *Responding to a Health Privacy Breach: Guidelines for the Health Sector*, retrieved from <https://www.ipc.on.ca/en/resources-and-decisions/responding-health-privacy-breach-guidelines-health-sector>.
[4] PHIPA Decision 155 at para 49.
[5] PHIPA Decision 110 at para 64.
[6] *PHIPA,* s 2.

with community agents as well as any documentation to formalize the relationship and grant necessary privileges. The custodian advised that prior to the incidents, they had no formal way of establishing the agency relationship and the requisite EMR access.

[26] Previously, community agents would obtain EMR access by filing out a request form which went directly to the custodian's third-party IT service provider, who would supply the agents with information necessary to install the EMR software. The agents would be scheduled to receive the necessary training, but the custodian relied on the agents to inform the custodian that they received the installation instructions. By then, the agents would have already received from the custodian's data management specialist the temporary passwords necessary to establish EMR access.

[27] The nurse was initially scheduled to complete her EMR training shortly upon onboarding, but it was postponed because the IT service provider supplied incorrect login credentials. Before completing the rescheduled training, however, the nurse received the correct information directly from the provider, then proceeded to set up the EMR software without informing the custodian's data management specialist. Based on information from the custodian, about a quarter of the inappropriate viewings occurred before the EMR training was completed.

[28] As a result, the nurse did not go through the standard onboarding process which would have included mandatory privacy training and signing the confidentiality agreement. These requirements were fulfilled after the breaches occurred.

[29] From the information provided, the fact that the nurse obtained EMR access without completing the privacy training and signing the confidentiality agreement appears to have been an isolated incident. However, in my view, this fact nevertheless demonstrates a gap in the custodian's onboarding process for community agents. More broadly, the circumstances highlight the need to formalize the custodian's relationship with community agents and clarify the agents' obligations and expectations with respect to the privacy and security of PHI in the custodian's custody or control.

[30] To address the above noted gap with respect to agents employed by partner communities, the custodian implemented a new internal policy on privacy and security training to formalize and strengthen the onboarding of community agents. The custodian communicated the policy and related procedures to the health directors from these communities in May 2024.

[31] According to this policy, for an employee of a partner community to become an agent for the custodian, the community's health director must formally request the custodian to provide the necessary EMR access for the employee. As a precondition for access, the employee must complete the necessary requirements including privacy and EMR training and signing of a confidentiality agreement. Furthermore, before EMR access is granted, approval must be signed by the community health director and verified by the custodian's director, with final approval by the custodian's privacy officer.

[32] According to the new procedure, the custodian's data management specialist must request the IT service provider for EMR access on behalf of any new user, rather than the request being made by the user themselves. The specialist does not provide login credentials until the user has satisfied the above noted requirements.

[33] In addition to the new policy, the custodian reviewed their list of EMR users and deactivated any inactive users, ensuring that the list is up to date with active users confirmed to have received privacy training and signed the confidentiality agreement.

[34] During this investigation, I asked the custodian about the active client list that was provided to the nurse on December 18, 2024, the day on which unauthorized disclosure of PHI occurred. The custodian advised that community health nurses would request lists of clients since the custodian works closely with them to provide continuity of care to patients in different communities. The custodian now requires that all requests for client lists from community agents receive approval from the custodian's privacy officer before they are released.

Protocol agreements with partner Indigenous communities

[35] The custodian advised that it has "protocol agreements" in place to manage their broader partnerships with Indigenous communities. At the time of the breaches, the custodian's agreement with the community at issue did not establish how the community employees would work as agents for the custodian.

[36] As remediation, the custodian undertook review of their existing protocol agreements with partner communities to clarify the privacy expectations and obligations between parties. According to the custodian, the agreements were revised to include references to the *Act* and ensure consistency with the custodian's obligations under the legislation, including the obligation with respect to the collection, use and disclosure of PHI. The agreements also stipulate that all agents receive privacy training and must follow the same privacy program as the custodian's employees, and that there is a clear communication plan and reporting expectation between the custodian and partner communities.

[37] The custodian also noted that they created a new data sharing agreement, a document which outlines the custodian's commitments about how it handles personal health information as part of providing their services to the partner communities. Among other things, the agreement highlights the custodian's commitment to privacy and security of patients' PHI pursuant to the *Act* and explains situations in which limited information may be shared for statistical or research purposes. The agreement also states that in delivering their services, the custodian respects the OCAP® principles[7] of

[7] OCAP® is a registered trademark of the First Nations Information Governance Centre (FNIGC). According to FNIGC, OCAP® is a tool to support strong information governance on the path to First Nations data sovereignty. These principles establish how First Nations' data and information will be collected, protected,

Indigenous data governance.

[38] The custodian advised that the revised protocol agreements and the new data sharing agreement will be presented to the Board of Directors for final approval in September 2025.

Audit of EMR access logs

[39] As part of their investigation, the custodian audited the nurse's EMR access history starting from the date of her onboarding. It was noted that while the audit identifies the patients whose charts are accessed, it does not identify the specific types of health records that the nurse viewed, unless the user specifically opens or prints a part of the patient chart.

[40] To address this gap and to improve the overall security of the EMR, the custodian implemented a documentation feature whereby the user accessing a patient chart would insert a text into a generated stamp to indicate the reason for the chart access.

[41] The custodian also noted that they now conduct scheduled audits and random audits as part of their privacy practice. As per their audit policy, all EMR users have designated locations in which they are to access information. A random audit may be triggered if suspicious activity is detected.

Confidentiality agreement

[42] An important administrative safeguard in protecting patients' PHI is requiring agents to sign on a regular basis a confidentiality agreement which require agents to acknowledge the privacy obligations and expectations, including the consequences of a privacy breach.[8]

[43] Previously, community agents were required to sign the confidentiality agreement only upon onboarding. In response to the breaches, the custodian amended their practice so that agents are required to sign the agreement upon onboarding and semi-annually.

[44] The confidentiality agreement includes a detailed confidentiality and non-disclosure undertaking with respect to information of personal, confidential and/or proprietary nature, including personal health information, which is described as any information about an identifiable individual such as name, date of birth and health card number. The undertaking includes the obligation to take all necessary precautions to keep the confidential information secure and to protect it from unauthorized use, reproduction

---

used, or shared. More information can be found on FNIGC website available online: <https://fnigc.ca/ocap-training/>.

[8] *See* Information and Privacy Commissioner of Ontario (January 2015), *Detecting and Deterring Unauthorized Access to Personal Health Information*, retrieved from <https://www.ipc.on.ca/en/resources-and-decisions/detecting-and-deterring-unauthorized-access-personal-health-information>.

or disclosure.

[45] The agreement requires the signee to comply with privacy laws and regulations, which apply to the collection, use and disclosure of personal information. Following discussions with the IPC, the custodian has agreed to improve the agreement by including specific reference to the *Act* and its definition of personal health information. The custodian committed to making this change by September 2025.

Privacy training

[46] The custodian provided the IPC with their orientation privacy training documentation. It addresses terms and concepts from the *Act*, such as the definition of PHI, the importance of patient confidentiality and the responsibilities and permitted activities of health information custodians and agents with respect to PHI. The documentation also addresses administrative, technical and physical safeguards implemented by the custodian to protect the PHI of patients, as well as the significance and consequences of privacy breaches.

[47] Following the breaches, the custodian completed additional training initiatives to increase privacy awareness within the organization and their partner communities. For example, the custodian launched a large-scale privacy training session involving the Community Health Directors, Community Health Nurses and other agents from partner communities to share the new formal procedure for granting EMR access and the obligations of community agents.

[48] In addition, between September 2024 and January 2025, the custodian implemented monthly privacy lunch and learns for employees and community agents to address specific privacy topics, such as consent, EMR access and audits, privacy safeguards, breaches and cybersecurity practices.

[49] Other remedial initiatives focused on establishing better communications with community gents to ensure that they are included in the custodian's privacy updates, monthly privacy newsletters and other privacy related resources. The custodian also conducts department specific privacy training, including regular meetings to discuss privacy issues as well as scheduled in-person privacy sessions.

[50] The custodian created physical binders containing privacy policies and forms related to consent, privacy notice, chart audit request, lockbox request form and information brochure. These binders have been placed in the clinic sites of respective communities, to reinforce privacy awareness for employees and community agents.

Privacy warning flag

[51] Privacy notices and warning flags in electronic record systems serve to remind custodians and their agents about their obligations to protect PHI and the potential consequences of accessing PHI in contravention of the *Act.* They may prevent or reduce

the risk of unauthorized access to PHI.[9]

[52] During this investigation, the custodian reported that their EMR did not contain any privacy warning that users view before accessing PHI. The custodian accepted the IPC's recommendation and implemented a privacy warning flag in the EMR. When a user logs into the EMR, they must now agree to a pop-up confidentiality acknowledgment which reads in part as follows:

> … I acknowledge the importance of protecting the confidentiality and integrity of any personal or personal health information to which I have access. I agree not to collect, use or disclose such information to any person or organization except as necessary in the course of providing my services.
>
> Further, I:
>
> > i. Acknowledge that I have received, read and understood [the custodian's] privacy policies.
> >
> > ii. Acknowledge that I received, read and understood the Confidentiality Agreement.
> >
> > iii. Agree that [the custodian's] privacy policies and supporting instructions form part of my terms of employment or my contract, and that any violation of this Security Acknowledgement and Confidentiality Agreement may result in disciplinary action, up to and including termination of employment, association or contract.
> >
> > iv. Agree that I will immediately notify the Privacy Officer(s) in the event that I become aware of any violation of [the custodian's] privacy policies, or accompanying instructions, including any unauthorized collection, use, disclosure, or disposal of personal health information, other than in accordance with [the custodian's] Privacy Policies, as amended from time to time.

Privacy policies

[53] The custodian advised that they maintain the following policies related to the privacy and security of personal health information:

- Privacy Policy
- Privacy Breach Protocol
- Withdrawal of Consent (Lockbox) Policy

[9] PHIPA Decision 110 at para 100.

- Safeguards for Client Information Policy
- Privacy Audit Policy
- Storage, Retention & Destruction of Health Records
- Privacy & Security Training
- Electronic Communication

[54] The custodian advised that the privacy policies are reviewed and revised annually. The policies were updated after the breaches and in October 2024, the custodian obtained from the community agents written acknowledgement that they had reviewed the updated policies. The custodian noted that their implementation of Privacy & Security Training (discussed above) and Email Communication policies was the most significant change to the organization's privacy program following the breaches.

CONCLUSION:

[55] The issue before me in this case is whether the custodian had reasonable safeguards in place at the time of the breaches to protect PHI of their patients.

[56] As discussed above, the custodian's practices related to the onboarding process, the EMR and the overall management of community agents were deficient in several ways. Previously, new agents were required to complete privacy training and sign a confidentiality agreement only once upon orientation. Further, the onboarding process allowed the possibility of new agents obtaining EMR access without first completing these requirements, as the breaches in this case demonstrated.

[57] As for the EMR, it did not display a privacy warning to users logging in to remind them of their privacy obligations when handling PHI. Further, the EMR's configuration did not allow audits to show the types of records a user accessed within a patient chart and the reasons for the access, thus impacting the quality of the audit results and the custodian's ability to track instances of unauthorized access.

[58] More broadly, the custodian did not have a way to formally establish the agency relationship with community agents. Notwithstanding the custodian's service model based on their partnership with the Indigenous community that employed the nurse, the custodian's protocol agreement with the community did not articulate how the community agents may work on behalf of the custodian.

[59] For these reasons, I find that, at the time of the breaches, the custodian did not take steps that are reasonable in the circumstances to ensure that PHI in their custody or control is protected, contrary to section 12(1) of the *Act.*

[60] Nevertheless, in response to the breaches, the custodian identified and addressed these gaps in their practices by adopting an array of significant improvements. The custodian established a new privacy and security training policy which improved and formalized the onboarding process for community agents and ensured the completion of privacy training and confidentiality agreement at onboarding and on a regular basis. The custodian also added safeguards to the EMR by implementing a privacy warning as well as a documentation standard requiring users to record their reasons for accessing patient charts.

[61] Furthermore, the custodian has completed various training initiatives with partner communities and community agents to provide education on the custodian's privacy policies and key concepts and obligations, reinforcing overall privacy awareness and culture for the community agents who work with the custodian.

[62] During this investigation, the custodian committed to further improving the confidentiality agreement signed by community agents to include reference to the *Act.* Finally, the custodian undertook review and revision of their contractual arrangements with partner Indigenous communities

[63] Given these remedial steps by the custodian, I am satisfied that the custodian has responded adequately to the privacy breaches in this case.

NO REVIEW:

Section 58(1) of the *Act* establishes the Commissioner's discretionary authority to conduct a formal review under the *Act,* as follows:

> The Commissioner may, on his or her own initiative, conduct a review of any matter if the Commissioner has reasonable grounds to believe that a person has contravened or is about to contravene a provision of this Act or its regulations and that the subject-matter of the review relates to the contravention.

In accordance with my delegated authority to determine whether a review should be conducted under section 58(1) of the *Act* and for the reasons set out above, I find that such a review is not warranted.

For the foregoing reasons, no further review of this matter will be conducted under Part VI of the *Act.*

Original Signed by: July 17, 2025

Francisco Woo
Investigator