

Important Notice Regarding Cybersecurity Incident

Nipigon District Memorial Hospital ("NDMH") is providing further information about the cybersecurity incident it first announced on September 15, 2026, with further information released on October 1, 2026. **See updates highlighted in yellow.**

What happened?

We first became aware of the incident on September 14, 2026. We immediately activated our incident response and business continuity procedures and engaged external cybersecurity experts.

While indications were initially unclear, theft of files from an NDMH file share is now confirmed. We have now analyzed the set of stolen files, which unfortunately includes patient information. Our electronic medical record was not affected.

Privacy notification

Based on our analysis, we are notifying patients of the following exposure.

Please note that the amount of information exposed varies by individuals. Not all individuals have had each listed data element exposed.

Groups of individuals who are likely affected	Information exposed includes*
Inpatients receiving services at NDMH between October 2021 and September 2026 Updated: Oct 13, 2026	Full name, Health Card Number, Date of Birth, Phone number, mailing address, Clinical Information
Physiotherapy outpatients admitted between April 2021 to March 2025	Full name, Health Card Number, Phone Number, Clinical Information
Diagnostic imaging outpatients admitted between September 2025 and September 2026	Full name, Procedure Performed, Provider Name
Telemedicine outpatients admitted between May 2024 and September 2026	Full name, Health Card Number, Address, Clinical Information
Emergency outpatients admitted between November 2023 and September 2026	Full name, Health Card Number, Date of Birth, Clinical Information, Next of Kin name (with phone number, mailing address, and e-mail address)
Assisted living outpatients admitted between September 2022 and September 2026	Full name, Health Card Number, Address, Phone Number, Emergency Contact name (with contact phone number and e-mail address)
Meals on Wheels outpatients admitted between January 2026 and September 2026	Full name, Address, Phone Number, Next of Kin name (with phone number and e-mail address)
Long term care residents who passed away between April 2018 and June 2026	Full name, Date of Death, Emergency contact name (with phone number, mailing address and email address)
Individuals who applied for employment at NDMH between March 2026 and September 2026	Full name, Address, Phone Number, E-mail Address, Job Application Materials

Volunteers/Students who worked at NDMH between January 2020 and September 2026	Full name, Address, Phone Number, E-mail Address, Results of Vulnerable Sector Check, COVID test result Updated: Oct 13, 2026
All visitors, staff, or other individual who attended the hospital and was screened for COVID from November 2020 to October 2022 Updated: Oct 13, 2026	Full name, COVID test results Updated: Oct 13, 2026

* "Clinical information" refers to medical history, diagnoses, treatment plan information, and provider names.

We will notify long-term care residents and next of kin, and a small number of affected patients by email or mail directly. If you are not identified above or do not receive a direct notification from us, we have not identified you as being affected by this incident.

Sensitive information related to staff working at NDMH employed by other agencies was not identified as being affected by this incident. Agency staff can reach out to their employer if they have further concerns. We have reported this matter to law enforcement and the Information and Privacy Commissioner of Ontario. You can learn about your entitlement to complain at <http://www.ipc.on.ca>, though we have reported this incident to the IPC and will provide it with our full cooperation.

Our analysis is ongoing. If we identify further exposure, we will identify affected individuals as appropriate and required by law.

What this means to affected patients

To be cautious, you should always watch for the following.

- Messages that say they are from NDMH when you weren't expecting them.
- Anyone asking you for personal or health information (like your address, date of birth, health card number, Social Insurance Number, or banking details).
- Emails, texts, or calls that sound urgent or pressure you to act fast.
- Links or attachments you did not ask for or did not expect.
- Names, phone numbers, or e-mail addresses that do not look right or feel different from usual.
- Websites that look odd or do not match the normal CarePoint Health website.

We also invite you to contact us at the email below, should you have any reason to believe your NDMH information has been misused.

What We Are Doing

We are sincerely sorry that this incident occurred and for the concern it may cause. Our organization was targeted by criminal actors whose actions run directly contrary to our values and the trust our community places in us. While we are deeply disappointed that this criminal activity has affected our patients, we want to be clear that we are responding decisively - working to secure our systems, protect information, and support law enforcement and other authorities in holding those responsible accountable.

If you have any questions about this notice, please contact privacy@ndmh.ca

NDMH CYBERSECURITY INCIDENT FAQ

What happened?

On Sept 14, 2026 an unauthorized person gained access to NDMH's computer systems. While indications were initially unclear, theft of files from an NDMH file share is not now confirmed.

How did this happen?

Our investigation is ongoing. When it is complete we hope to have reliable information about how this happened. In the interim, based on the steps we have taken together with experts we are confident in the security of our network.

Who may be affected?

The incident affects patients, long-term care residents, employees, students, and volunteers. For information about affected individuals that we have made public, see www.ndmh.ca. Some individuals will also be directly notified.

When did you learn about the incident?

NDMH became aware of the incident on September 14, 2026. We immediately activated our incident response and business continuity procedures and engaged external cybersecurity experts.

Why are you publishing a notification?

NDMH is publishing this notice in the interest of transparency and so that potentially affected individuals are aware of the incident.

What is the risk to me?

The risk of identity fraud is unfortunately a common reality today, whether personal information is compromised through a privacy breach, phishing attack, malware infection, or other means. There are practical steps you can take to protect yourself, and we are providing support to assist employees given the nature of information that was exposed.

Is there anything I should do?

Remain alert for suspicious emails, text messages, or telephone calls that request personal information or claiming to relate to health coverage, government programs, or identity verification. Always verify the identity of anyone requesting personal information. Employees who have received codes for credit monitoring services should enrol.

Has this incident been reported to law enforcement or the Privacy Commissioner?

Yes, we have reported this matter to law enforcement and the Information and Privacy Commissioner of Ontario. You can learn about your entitlement to complain at <http://www.ipc.on.ca>, though we have reported this incident to the IPC and will provide it with our full cooperation.

Are you providing credit monitoring services to patients?

No. Based on the patient information involved and our assessment that the risk of misuse is low, we have concluded that credit monitoring services for patients are not warranted in the circumstances.

What are you doing in response?

We are responding decisively – working to secure our systems, protect information, and support law enforcement and other authorities in holding those responsible accountable. We will also monitor the situation and assess whether the risk has changed.