MANITOBA OMBUDSMAN

PERSONAL HEATH INFORMATION ACT INVESTIGATION REPORT

Medical Clinic in Winnipeg

Unauthorized Collection, Use, Disclosure and Security of Information

CASE# MO-05481
Public Report

Issue Date:
September 4, 2025

Provisions considered:
PHIA – 13(1), 18(2), 21(1), 22(1), 63(1)(d), 63(1)(f), 63(2)(b),
PHIA Regulation – 4(1), 4(4), 5, 6, 7

SUMMARY

In January of 2022, a privacy complaint was received by our office in relation to an employee of a Winnipeg-based medical clinic accessing personal health information (PHI) without authorization.

Our office investigated the complaint and determined that the employee created falsified medical records of the complainant for the purpose of being able to access linked records in another system, and that the collection, use and disclosure of the complainant's PHI was not authorized. Therefore, the complaint is supported.

Our office initiated a prosecution of the employee under The Personal Health Information Act (PHIA). The employee pleaded guilty to unauthorized use of the complainant's PHI.

The employee's employment with the clinic was terminated during this investigation. We are satisfied that the clinic appropriately addressed the privacy breach.

INTRODUCTION

This report concerns an investigation of a complaint under The Personal Health Information Act (PHIA), relating to the unauthorized access of the personal health information (PHI) of the complainant by an employee of a Winnipeg-based medical clinic.

The clinic is the trustee being investigated in this matter as it was their employee who accessed the PHI and the breach involved their electronic medical record system (EMR). The EMR includes a portal to another system, called eChart, which contains the complainant's PHI that was the subject of this breach.

eChart is an electronic system that pulls together information, including prescriptions, lab results, immunizations and x-ray reports, from other electronic systems in Manitoba.[1] Shared Health, Manitoba's provincial health authority, operates eChart, and health-care providers can request access privileges to eChart for themselves and their staff.

As the PHI that was accessed was contained within eChart, we notified Shared Health of the breach and investigation by our office.

INVESTIGATION

On January 24, 2022, the complainant contacted our office to ask questions about making a complaint about a breach of their privacy. The complainant indicated they requested an audit of their eChart records and that the records showed that an individual had accessed their personal health information. On January 27, 2022, they made a complaint and an investigation file was opened.

Complaint Investigation

As Shared Health operates the eChart system and eChart tracks who has access and where they are accessing information from, we contacted Shared Health and asked them for information on where the individual was employed. Shared Health informed our office that the individual was employed at a Winnipeg-based medical clinic.

[1] eChart Manitoba, "Home Page", (2025, February), online (website): <https://echartmanitoba.ca/>

Our office also requested an audit of the employee's accesses of the complainant's eChart record from Shared Health, which we received. Our office contacted the clinic and informed them of the complaint and requested that they conduct an audit of the employee's access of the complainant's patient file in their electronic medical record (EMR) system.

The clinic advised our office that although there was a patient file under the complainant's name in their EMR, the complainant was never a patient at the clinic and had never attended the clinic. The clinic informed us at this time that the employee (now former employee) was no longer employed with their clinic.

Our investigation determined that the former employee created a fake patient file for the complainant in the clinic's EMR and then used that patient file to click through the eChart portal to gain access to the complainant's eChart records where their PHI was located.

Between December of 2020 and April of 2021, the employee accessed the complainant's PHI 32 times on 26 separate dates, with some days having multiple accesses. The employee accessed a significant amount of PHI for the complainant, including:

- diagnostic imaging reports, such as x-rays, CT scans, MRIs
- lab reports, such as blood work, urine results
- test history
- hospital visits
- medications
- enrolment status, which includes information about medical professionals that a patient attends
- pathology reports
- annual review tabs, which is any encounter, lab, or imaging result and includes a date with a hyperlink to any related documents

Under PHIA, a "use" of personal health information includes situations when the trustee or its employees access records and information held by the trustee. PHIA states that PHI may only be used for an authorized purpose.

Subsection 21(1) of PHIA sets out when trustees and their employees are authorized to use PHI:

> ***Restrictions on use of information***
> ***21(1)*** *A trustee may use personal health information only for the purpose for which it was collected or received, and shall not use it for any other purpose, unless*
>
> *(a) the other purpose is directly related to the purpose for which the personal health information was collected or received;*
>
> *(b) the individual the personal health information is about has consented to the use;*
>
> *(c) use of the information is necessary to prevent or lessen*
>
> *(i) a risk of harm to the health or safety of a minor, or*
>
> *(ii) a risk of serious harm to the health or safety of the individual the information is about or another individual, or to public health or public safety;*
>
> *(c.1) the information is demographic information about an individual, or is his or her PHIN, and is used to*
>
> *(i) confirm eligibility for health care or payment for health care, or*
>
> *(ii) verify the accuracy of the demographic information or PHIN;*
>
> *(c.2) the information is demographic information about an individual and is used to collect a debt the individual owes to the trustee, or to the government if the trustee is a department;*
>
> *(d) the trustee is a public body or a health care facility and the personal health information is used*
>
> *(i) to deliver, monitor or evaluate a program that relates to the provision of health care or payment for health care by the trustee, or*
>
> *(ii) for research and planning that relates to the provision of health care or payment for health care by the trustee;*
>
> *(d.1) the information is used for educating individuals respecting the provision of health care, including*

(i) employees and agents of the trustee,

(ii) students training to be health professionals, and

(iii) health professionals who have been granted privileges to provide services at a health care facility operated by the trustee;

(e) the purpose is one for which the information may be disclosed to the trustee under section 22; or

(f) use of the information is authorized by an enactment of Manitoba or Canada.

In this case, the employee created a fake patient profile of the complainant for the sole purpose of accessing the complainant's PHI that existed in the linked eChart system. The complainant was not a patient of the clinic and the clinic never provided health care to the complainant. PHIA also sets out requirements for the collection of PHI:

Restrictions on collection

13(1) *A trustee shall not collect personal health information about an individual unless*

(a) the information is collected for a lawful purpose connected with a function or activity of the trustee; and

(b) the collection of the information is necessary for that purpose.

A "collection" of PHI occurs any time a trustee takes custody of or has control over PHI. In this case, the PHI of the complainant was collected when the employee created the fake patient file. The employee had no lawful purpose for collecting the complainant's PHI.

Lastly, PHIA limits the disclosure of PHI.

Individual's consent to disclosure

22(1) *Except as permitted by subsection (2), a trustee may disclose personal health information only if*

(a) the disclosure is to the individual the personal health information is about or his or her representative; or

(b) the individual the information is about has consented to the disclosure.

During our investigation, the complainant explained that they first suspected their privacy was breached because of comments made by a third party about the complainant's health-care matters. This third party should not have had access to the complainant's PHI. This caused the complainant to request an audit of their eChart records and to then contact our office.

The former employee later admitted in court that they had provided the complainant's PHI to the third party, who was the former employee's friend at the time. The former employee explained that they created the fake patient file and accessed the complainant's eChart records at the request of the third party.

The former employee did not have the consent of the complainant to disclose their PHI. An individual's PHI can only be disclosed without the individual's consent in limited circumstances, none of which would apply in this case. Given these facts, our office found that the collection, use and disclosure of the complainant's PHI was not authorized under PHIA.

Prosecution Under PHIA

Based on the evidence gathered during our complaint investigation, our office determined that the actions of the employee met the requirements of an offence under PHIA. We provided the relevant evidence to the Manitoba Prosecution Service (Prosecutions) for its review and decision on whether this matter would be prosecuted.

Prosecutions determined that there was sufficient evidence to proceed with an offence prosecution in relation to the breach of the complainant's PHI.

On January 29, 2024, the Ombudsman filed three charges against the former employee under clauses 63(1)(d), 63(1)(f) and 63(2)(b) of PHIA.

Offences
63(1) *Any person who*

(d) obtains another person's personal health information by falsely representing that he or she is entitled to the information;

(f) knowingly falsifies another person's personal health information;

is guilty of an offence.

Offence by employee, officer or agent
63(2) *Despite subsection 61(2), a person who is an employee, officer or agent of a trustee, information manager or health research organization and who, without the authorization of the trustee, information manager or health research organization, wilfully*

(b) uses, gains access to or attempts to gain access to another person's personal health information;

is guilty of an offence.

On July 23, 2024, the former employee pleaded guilty to the charge of unauthorized use of PHI under clause 63(2)(b) of PHIA and received a fine of $7,000.00.

Our office does not issue investigation reports for complaints while a prosecution is ongoing. While the investigation and the issuing of our report was paused, our office provided updates on the prosecution to the parties involved.

Review of the Clinic's Policies, Procedures and Security Safeguards

Our investigation also reviewed the steps the clinic took to address the breach, and any measures taken by the clinic to limit the risk of further breaches. Specifically, we reviewed the policies, procedures, and security safeguards of the clinic.

Our office requested copies of the clinic's policies and procedures for privacy breaches, audits, and any other policies related to PHIA. We also reviewed the steps taken by the clinic to address the privacy breach.

Access to PHI

PHIA and The Personal Health Information Regulation (the regulation) require trustees to have controls which limit who can use PHI, and when and how much PHI they can use. Subsection 18(2) sets out the requirement for these controls under PHIA:

Specific safeguards
18(2) *Without limiting subsection (1), a trustee shall*

(a) implement controls that limit the persons who may use personal health information maintained by the trustee to those specifically authorized by the trustee to do so;

(b) implement controls to ensure that personal health information maintained by the trustee cannot be used unless

(i) the identity of the person seeking to use the information is verified as a person the trustee has authorized to use it, and

(ii) the proposed use is verified as being authorized under this Act;

Section 5 of the regulation requires trustees to determine what PHI each of their employees is authorized to access:

Authorized access for employees and agents

5 *A trustee shall, for each of its employees and agents, determine the personal health information that he or she is authorized to access.*

One of the first steps the clinic took after being informed of the privacy breach was to remove the employee's access to the clinic's EMR and eChart. The clinic also updated all of its employees' eChart access privileges[2] and reviewed all access to its EMR to ensure that the access of any former employees was removed and that only current employees had access to patient PHI.

During our investigation we requested information from the clinic about the controls it has in place for access to both its EMR and eChart. The clinic indicated that it uses the following controls to verify the identity of the employees accessing patient PHI and limit the amount of PHI that employees can access to only the information necessary:

- Verification controls:

  - each employee has their own username and password
    employees are required to change their password every 8 weeks
  - Two-factor authentication is required for all logins to the clinic's EMR

[2] Privacy Officers for medical facilities have the ability to add and remove eChart access for employees and set the level of access for each employee.

- Access controls:

    - employees must request new or updated access to either the EMR or eChart, from the clinic's privacy officer
    - the privacy officer determines and sets the level of access for each employee

PHIA Pledge of Confidentiality

The regulation requires all trustees to ensure that their employees sign a pledge of confidentiality that includes an acknowledgement that they are bound by the requirements of PHIA and are aware of the consequences for breaching these requirements.

This requirement is set out in section 7 of the regulation:

> ***Pledge of confidentiality for employees***
> ***7*** *A trustee shall ensure that each employee and agent signs a pledge of confidentiality that includes an acknowledgment that he or she is bound by the policy and procedures referred to in section 2 and is aware of the consequences of breaching them.*

The clinic provided a copy of its pledge of confidentiality which states that the individual understands that the PHI they have access to is private and confidential and that they understand that they are bound by the requirements of PHIA, the regulations and the policies and procedures of the trustee.

The pledge also states that the individual agrees not to collect, use, disclose, or destroy PHI except as authorized by PHIA, the regulations and the trustee's policies and procedures.

Lastly, the pledge states that the individual acknowledges that a failure to comply with PHIA, the regulation or the policies and procedures of the trustee could result in disciplinary action up to and including termination, a report being made the individual's professional regulatory body and could result in a prosecution under PHIA.

The employee had signed a pledge on October 5, 2020, before they started employment at the clinic. This was the only pledge they signed before the privacy breach began in February of 2021.

The clinic indicated that employees are now required to review and sign a pledge of confidentiality every year. The clinic also indicated that employees are provided with a copy of the clinic's PHIA policy at the same time to ensure that staff understand their responsibilities in relation to PHIA and PHI.

Auditing Access to PHI

Regular audits of access to PHI support transparency and accountability in the use of PHI, which enhances public trust and confidence in the health-care system's ability to manage PHI and protect privacy.

Subsection 4(1) of the regulation sets out requires trustees to create records of user activity:

> ***Additional safeguards for electronic health information systems***
> ***4(1)*** *In accordance with guidelines set by the minister, a trustee shall create and maintain, or have created and maintained, a record of user activity for any electronic information system it uses to maintain personal health information.*

Records of user activity are records showing who accessed the PHI of an individual and when. Subsection 4(4) of the regulation requires trustees to audit those records of user activity:

> ***4(4)*** *A trustee shall audit records of user activity to detect security breaches, in accordance with guidelines set by the minister.*

Audits of records of user activity help trustees know when, how and by whom PHI is used. The Minister of Health has established a set of guidelines (the guidelines) which include guidelines for conducting audits of systems that contain PHI, as required by subsection 4(4) of the regulation. The guidelines require trustees to have a process for how audits are completed.

The guidelines also set out the several types of privacy-related audits that should be done. These include random audits, audits based on specific triggers, such as when an employee accesses the PHI of someone with the same last name or an individual who has appeared in the media and focused audits that are conducted when the trustee identifies a specific issue that needs to be investigated, such as when a complaint of unauthorized use is made.

PHIA, the regulation, and the guidelines all require trustees to ensure that systems containing PHI are being audited and that the trustee has a set process for how that occurs.

Upon learning of the breach, the clinic audited the employee's access of their EMR from the employee's start date in November of 2020, to the end of April 2021. The clinic's EMR audits show the date a file was created, who created it and every time that file was accessed. The clinic used the audit to determine that the employee created a fake patient file and had used that file to access the PHI of the complainant.

The EMR audit showed the employee was the only employee of the clinic to access that file other than the clinic's privacy officer, who only accessed the complainant's file to generate an audit of that file at our request.

Prior to the privacy breach, the clinic would conduct random audits of employee access at various times but did not have a strict schedule for doing so. The clinic would also conduct audits if they received a privacy complaint or were otherwise notified of a specific concern.

After this incident, the clinic began auditing their EMR once each month by randomly selecting a patient file and reviewing the access of the file by its employees to ensure all access was authorized.

In relation to eChart, Shared Health is the trustee responsible for auditing access to eChart. Shared Health conducts random audits and sends those to site privacy officers for review. Shared Health also audits based on accessing PHI of individuals with specific triggers, such as same last name, co-workers or individuals with high public profiles. These audits are also sent to the site privacy officer for review.

Privacy and Security Policies

PHIA, the regulation and the guidelines require trustees to have policies and procedures related to privacy and security. These policies and procedures should address topics including security measures and safeguards to protect PHI, privacy breaches, and the collection, use, disclosure, retention, and destruction of PHI.

The clinic provided our office with information about its procedures and safeguards related to protecting PHI. Several of those procedures and safeguards include measures that reduce the risk of a similar breach occurring in the future, including requiring employees to review "Ten Tips for Addressing Employee Snooping"[3] to promote a culture of privacy.

Employees are also required to review and sign a new pledge of confidentiality every year. The pledge includes a requirement that employees only collect, use and disclose PHI as authorized by PHIA and in compliance with the clinic's policies.

After learning of the breach, the clinic also started doing random audits of its employees' access of PHI and random audits of patient files. This measure will assist the clinic in identifying potential breaches sooner and allow the clinic to more quickly address privacy issues, which will assist in limiting the risk of harm caused by a privacy breach.

Our office asked the clinic whether it had policies related to privacy, PHIA and its requirements. The clinic indicated that while the above procedures and safeguards are included in its general policy manual, it does not have any written PHIA and privacy policies that meet the requirements of PHIA, the regulation and the guidelines.

Our office provided the clinic information on what policies trustees are required to have and explained how having these policies is an essential part of a trustee's privacy program.
The clinic indicated that they understood the importance of having these policies and undertook to create and implement the required policies. The clinic also agreed to provide our office with updates on its progress with this work.

[3] "Ten Tips for Employee Snooping" is a guidance document produce by the Manitoba Ombudsman and is available on our website at https://www.ombudsman.mb.ca/resource/ten-tips-for-addressing-employee-snooping/

Employee PHIA Training

In addition to policies, procedures and safeguards, trustees can also promote a culture of privacy by providing regular PHIA training to employees. Section 6 of the regulation requires trustees to provide ongoing training to their employees.

> ***Orientation and training for employees***
> ***6*** *A trustee shall provide orientation and ongoing training for its employees and agents about the trustee's policy and procedures referred to in section 2.*

The clinic advised that following the discovery of the breach, a refresher was delivered to all employees on PHIA privacy requirements. The clinic also indicated that it will now provide annual training to employees on the requirements of PHIA and their responsibilities when accessing PHI. The clinic's privacy officer has also been providing regular reminders to employees to be mindful of their accesses of PHI in the clinic's EMR and eChart.

The clinic also encourages its employees to review a training video, created by Shared Health, on the use of eChart, "eChart 2022 Navigation Training Video" and reminds its employees that their access of PHI could be audited randomly or in the event of a suspected breach.

Lastly, the clinic sends regular reminders to employees to ensure that their computer screens are locked before patients are placed in an exam room and that if employees need new or updated access to eChart, they need to speak with the privacy officer.

CONCLUSION

Given our findings that the collection, use and disclosure of the complainant's PHI was unauthorized, the complaint is supported.

During the course of our investigation, the clinic took several steps to address the gaps in its privacy practices, reduce the risk of future privacy breaches and increase its ability to detect potential privacy breaches sooner. This included beginning regular audits of employee access and patient files, requiring yearly confidentiality pledges and privacy training for its employees, and undertaking to create written policies as required by PHIA.

Based on the steps taken by the clinic during the investigation, our review of the clinic's current privacy and security practices and the clinic's commitment to creating and implementing the required privacy policies, our office is satisfied that the clinic appropriately addressed the privacy breach.

This report concludes Manitoba Ombudsman's review of this matter.

Available in alternate formats upon request.

MANITOBA OMBUDSMAN
300 - 5 Donald Street, Winnipeg, MB R3L 2T4
204-982-9130 | 1-800-665-0531 | ombudsman@ombudsman.mb.ca
www.ombudsman.mb.ca