Manitoba Ombudsman

REPORT UNDER

THE PERSONAL HEALTH INFORMATION ACT

CASE 2018-0195

WINNIPEG REGIONAL HEALTH AUTHORITY

PRIVACY BREACH: USE OF PERSONAL HEALTH INFORMATION

PROVISIONS CONSIDERED: 20(1), 20(2), 20(3), 21

REPORT ISSUED ON OCTOBER 16, 2020

SUMMARY: A nurse at Grace General Hospital inappropriately accessed 1756 patient records in the Winnipeg Regional Health Authority (WRHA) Emergency Department Information System (EDIS). The nurse accessed the EDIS records by using login credentials that she had obtained while working in an emergency department at a different employer, Seven Oaks General Hospital. At the time the records were accessed, the nurse was not providing care to emergency department patients at Grace General Hospital. Accessing and viewing such records without an employment need to do so is an unauthorized use of personal health information and is considered a privacy breach. Our review of the WRHA investigation and response found that the WRHA took reasonable and appropriate steps to promptly address this breach. The WRHA considered requesting a suspension of the nurse's EDIS access while its investigation continued, but concluded that it could not appropriately do so until the investigation was completed.

We acknowledge the need for a comprehensive audit of user access to be undertaken as part of a complete privacy breach investigation. However, in this case the suspicion of unauthorized use could have been confirmed through an audit of recent access to EDIS, enabling a quicker decision about the nurse's access while a comprehensive audit was ongoing. This approach would strengthen the protection of personal health information and ensure that personal health information is used only for authorized purposes.

BACKGROUND

The Winnipeg Regional Health Authority (WRHA) is a personal health information trustee for the purposes of the Personal Health Information Act (PHIA or the act). In Manitoba, all trustees and their employees who collect and maintain personal health information are required to comply with the provisions of PHIA with regard to protecting personal health information from risks such as unauthorized use and disclosure.

On March 16, 2018, a WRHA employee working on a ward at Grace General Hospital noted what appeared to be a colleague's inappropriate use of the Emergency Department Information System (EDIS) while on shift. The first employee was aware that access to EDIS was not required for the colleague's health-care delivery role in that unit. This use of EDIS would not be authorized under PHIA.

The colleague in question was a nurse who also worked on a casual basis in the Emergency Department of Seven Oaks General Hospital (SOGH). As a result of this casual work at SOGH, she had been provided with login credentials to access EDIS, an electronic patient record which contains information pertaining to current and historical emergency department visits within the WRHA. That same day the first employee reported her concerns about her colleague's EDIS use to their manager and the Grace General Hospital privacy officer was informed.

The WRHA immediately began an investigation. As a result of its investigation, the WRHA determined that EDIS records for 1756 individuals had been accessed (used) without the required authority under PHIA. The nurse in question was not providing health care to these patients and, therefore, had no need to know the personal health information of these patients. The WRHA reported the unauthorized use to the ombudsman, which conducted a review of the WRHA's response to this privacy breach.

Early in its inquiries the WRHA notified the College of Registered Nurses of Manitoba (CRNM) about the investigation of this privacy breach by one of the college's members and the college was involved throughout. In the course of obtaining additional information further to the CRNM investigation, a deeper analysis of the nurse's user activity in EDIS was made. This second look at the audit uncovered the fact that on 19 occasions the nurse in question (despite her assurances to the contrary) had searched for specific individuals by name. Seven of those searches successfully found corresponding records for five distinct individuals (one of whom had since died).

GENERAL DUTIES OF PERSONAL HEALTH INFORMATION TRUSTEES UNDER PHIA

Subsection 20(1) of PHIA sets out the responsibilities of personal health information trustees regarding the use of personal health information. Simply put, no trustee (or their employee) shall use personal health information unless that use is authorized by the act. It reads:

> ***General duty of trustees re use and disclosure***
> ***20(1)*** *A trustee shall not use or disclose personal health information except as authorized under this Division.*

Generally speaking the personal health information of patients is collected for the purpose of providing health care to them and the information can be used for that purpose or another purpose or purposes if authorized under PHIA. Section 21 of PHIA describes the circumstances under which the use of personal health information is authorized:

> ***Restrictions on use of information***
> ***21*** *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 a serious and immediate threat to*
> *(i) the health or safety of the individual the information is about or another individual, or*
> *(ii) 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;*

(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.

Subsection 20(2) of PHIA states that each use of personal health information must be limited to only what is necessary to accomplish the purpose for which the information is used and subsection 20(3) states that use must be limited to those employees who require the personal health information for the performance of their job-related responsibilities, as follows:

Limit on amount of information used or disclosed
20(2) *Every use and disclosure by a trustee of personal health information must be limited to the minimum amount of information necessary to accomplish the purpose for which it is used or disclosed.*

Limit on the trustee's employees
20(3) *A trustee shall limit the use of personal health information it maintains to those of its employees and agents who need to know the information to carry out the purpose for which the information was collected or received or to carry out a purpose authorized under section 21.*

OUR REVIEW OF THE RESPONSE TO THE BREACH BY THE WRHA

The Manitoba Ombudsman practice note "Key Steps in Responding to Privacy Breaches…" [1] provides guidance to trustees about how to respond when a privacy breach has occurred. The four keys steps in responding to a breach are:

1) Contain the breach.
2) Evaluate the risks associated with the breach.
3) Notify affected individuals and others.
4) Prevent further breaches.

We reviewed the WRHA's response to the breach in relation to these key steps.

Containment

The first step in responding to a privacy breach is to take immediate, common sense steps to limit the breach. On receiving a report about the nurse's suspicious activity in EDIS on March 16, 2018, (a Friday) the nurse's manager responded and questioned the nurse about her use of EDIS on March 19, 2018 (the following Monday). As access to EDIS was not required for the nurse's health care delivery role (and, therefore, not authorized) she was cautioned not to use her

[1] Available online at https://www.ombudsman.mb.ca/info/privacy-breaches.html.

EDIS login credentials while working at Grace General Hospital. The nurse was also instructed to redo her PHIA training. As explained to our office by the WRHA, this employee provided her manager with assurances that she would no longer use her EDIS login credentials to access EDIS while working on a ward at Grace General Hospital.

On being made aware of this situation by the nurse manager, the nurse's area director and the Grace General Hospital privacy officer concluded that it would be appropriate to audit the nurse's activity in EDIS. On March 21, 2018, the WRHA requested a three-month audit of user activity in EDIS for the nurse in question from Manitoba eHealth[2]. The audit was provided to the WRHA on March 27, 2018, and a review of the results was completed by the Grace General Hospital privacy officer on April 9. The privacy officer concluded that the nurse in question had misused her EDIS login credentials while on shift at Grace General Hospital, including after meeting with her manager on March 19, 2018. The nurse's access to data systems was suspended on April 10, 2018.

On April 12, 2018, a meeting took place between the nurse in question, her union representative, WRHA human resources staff and the chief nursing officer. The nurse was questioned about her use of EDIS and she admitted viewing patient information in EDIS while on duty at Grace General Hospital. The nurse explained that she had an interest in emergency medicine and had viewed the patient records to expand her knowledge. The nurse stated that she did not target specific individuals but rather searched all records for interesting cases. She stated that she did not copy any information and did not disclose the personal health information she viewed to anyone.

A second and more comprehensive audit of user activity spanning the entire length of the nurse's tenure at Grace General Hospital was requested and delivered on April 25, 2018. As a result, the WRHA concluded that the nurse's activity in EDIS while at Grace General Hospital, which was not required for her professional duties there, took place without the authorization of the trustee. As a result of its investigation and audit of the nurse's use of EDIS, the WRHA concluded that the nurse had accessed the personal health information of 1756 individuals. This included 138 individuals who had since died and 37 minors. This is a breach of the requirements of PHIA.

The nurse in question is no longer employed by the WRHA.

Our office observed that there was a suspicion that the nurse in this case was misusing her access to EDIS as early as March 16, 2018. In our view, given that there was a suspicion of inappropriate use and the ability to access EDIS was not required for the nurse's employment at Grace General Hospital, the WRHA could have considered suspending her access to EDIS while

[2] Manitoba eHealth is now known as Digital Health, a Shared Health Manitoba service.

the investigation was ongoing rather than waiting for the audit results. Our office asked the WRHA why this was not done.

The WRHA explained that the nurse in question had two separate positions with two distinct health-care organizations. In this case, the nurse's EDIS credentials were authorized by SOGH and necessary for her casual position there. To remove the nurse's ability to access EDIS would prevent her from accepting shifts at SOGH with the effect of suspending her from that position before any breach investigation was concluded.

In this case, it was later discovered that the nurse continued to abuse her EDIS access even after she was warned about unauthorized use of EDIS by her manager. This illustrates the risk of allowing continued access to personal health information in electronic systems when unauthorized use of the system is suspected. Our office acknowledges that if an employee needs the access to a system to work, to remove access without having firm evidence of unauthorized use would be unfair. However, in our view it would have been possible to confirm the suspicion of unauthorized access to EDIS by auditing and reviewing a smaller portion of the three-month audit of user access (for example, one or two weeks of access) rather than waiting for a review of the nurse's entire three-months of access to be completed. If unauthorized access was confirmed following the shorter audit and review, the nurse's access to EDIS could be temporarily removed with cause pending completion of the entire three-month access audit.

Risk Assessment

An assessment of the risks associated with a breach first involves a determination as to what personal or personal health information was involved. According to information provided to our office by the WRHA, the main screen of EDIS is a status board which displays personal health information about a patient's emergency room (ER) visit including patient name, age, chief complaint (main reason for patient's visit), the length of time the patient has been registered in the ER and the patient location.

From the main screen, the EDIS user can click on tabs which give access to more detailed personal health information[3] as follows:

- **Orders Tab**: Information about instructions given for types of care such as diagnostic imaging, intravenous (IV) therapy, special nursing, oxygen, transfusions or spiritual care.
- **Results Tab**: Information about test results (i.e. blood tests, diagnostic imaging)
- **Patient Info Tab**: Information about the patient such as special alerts, allergies, emergency contacts, detailed patient demographics, other health issues, insurance and visit history (list of all ER visits).

[3] The examples provided here are not exhaustive but are intended to illustrate the type of information available on the EDIS system.

• **Documents Tab**: The types of documents which can be viewed include initial assessment, summaries (i.e. assessment, discharge), patient history, consult requests, operative notes, procedure notes and Workers Compensation Board (WCB) notes.
• **Flowsheet Tab**: Flowsheets which can be viewed include care and assessment, vital signs and registered nurse (RN) reassessment.
• **Clinical Summary Tab**: Includes information about care plans, mobility assessment, wounds, infusions and catheters, pacemaker, malnutrition screening and active orders.

Clearly, the records in EDIS contain detailed personal health information, some of which is highly sensitive.

As set out in our practice note "Key Steps in Responding to Privacy Breaches under FIPPA and PHIA" the risk of possible harm from a privacy breach ranges from little to none (low risk) to a threat to physical safety or damage to reputation (high risk), as follows:

Low	Medium	High
▪ No foreseeable harm from the breach	▪ Loss of business or employment opportunities ▪ Hurt, embarrassment, damage to reputation or relationships ▪ Social/relational harm ▪ Loss of trust in the public body/trustee ▪ Loss of public body/trustee assets ▪ Loss of public body/trustee contracts or business ▪ Financial or legal exposure to public body/trustee	▪ Security risk (ex. physical safety) ▪ Identity theft or fraud risk ▪ Hurt, embarrassment, damage to reputation may also be high risk depending on the circumstances ▪ Risk to public health or safety

With respect to this breach, potential risks identified by our office include embarrassment to individuals if their personal health information becomes known by other people who are not involved in providing their health care. Other risks include loss of business or employment opportunities as well as social and relational harm. Loss of patient trust in the ability of the WRHA to protect personal health information is also possible.

As a result of a further review of the audit of user activity conducted during the course of its investigation, the WRHA determined that on 19 occasions the nurse in question had searched for specific individuals by name. Seven of those searches successfully found corresponding records for five distinct individuals (one of whom had since died). The WRHA explained that it asked for and received assurances from the nurse in question that no information from the EDIS

records she accessed was disclosed to anyone else and no copies were made. There is no evidence to date that any personal health information was disclosed inappropriately outside the workplace. We note, however, that a trustee can never be completely sure that a disclosure has not taken place or will not take place in the future. The WRHA was unable to further question the nurse about her motives for the specific searches as she was no longer in their employ when this was determined.

Notification

PHIA and FIPPA do not require a trustee or public body to notify individuals whose personal or personal health information has been inappropriately collected, used or disclosed, even if there is a real risk of significant harm to the individuals.

Our office recommends that trustees and public bodies assess the potential risk of harm to affected individuals. Generally, the more sensitive the information the greater the risk of harm to an individual should the information become known. In general, a medium or high-risk rating should result in notification to the affected individuals.

A key consideration in deciding whether to notify, and what form the notification should take, should be whether notification is necessary in order to avoid or mitigate harm to an individual whose personal health information has been inappropriately collected, used or disclosed. As explained in our practice note, there may be other factors that influence a decision to notify individuals, such as wanting to be transparent about the breach. Our practice note sets out considerations in determining whether to notify individuals affected by a breach:

- **Legislation requires notification**: Is the public body or trustee covered by legislation that requires notification of the affected individual? Note that FIPPA and PHIA do not require notification.
- **Contractual obligations require notification**: Does the public body or trustee have a contractual obligation to notify affected individuals in the event of a privacy breach?
- **Risk of identity theft or fraud**: Identity theft or fraud is a concern if the breach includes information such as names in conjunction with SIN, credit card number, driver's licence number, Personal Health Identification Number (PHIN), or any other information that can be used for fraud by third parties (ex: financial).
- **Risk of physical or mental harm**: Does the privacy breach place any individual at risk of physical or mental harm, stalking or harassment?
- **Risk of hurt, embarrassment or damage to one's reputation**: Could the privacy breach lead to hurt, embarrassment or damage to an individual's reputation? This type of harm can occur with the loss of information such as mental health records, medical records or disciplinary records.

• **Risk of loss of business or employment opportunities**: Could the privacy breach result in damage to the reputation of an individual, affecting business or employment opportunities?
• **Intentional breach**: In the case of an intentional breach, the affected individual may be in the best position to assess risks and take steps to mitigate them. The perpetrator of the breach may not fully disclose their motivation or their relationship to the individual (ex: ex-partner, family member, neighbour).

The WRHA decision to notify those individuals affected by this privacy breach was taken following its assessment of the risks associated with the breach. Based on the sensitivity of the personal health information in question, we are of the view that the unauthorized use of this information presented a real risk of significant harm to individuals and the WRHA's decision to notify the affected individuals was appropriate. The trustee also considered the form that notification would take. In this case, the WRHA determined that it was necessary to notify by letter those individuals whose personal health information had been accessed without authority.

On May 1, 2018, 1618 notification letters (dated April 26, 2018) were sent by the WRHA to all living persons[4] whose EDIS record was viewed by the nurse using her EDIS login. Additionally, a news release confirming that a privacy breach of the EDIS records of 1756 individuals had occurred was also issued by the WRHA on the same day.

The WRHA provided our office with a copy of its notification letter. We observed that patients were informed that a nurse employed by the WRHA had engaged in an unauthorized use of their personal health information as maintained in the EDIS system and the WRHA apologized for the privacy breach. The WRHA notification letter explained:

- the unauthorized use took place while the nurse was working at a separate WRHA site unrelated to emergency departments
- the use was a breach of PHIA, which limits the use of personal health information by WRHA employees to that which is required to perform their job
- that the nurse did not print, copy or retain any of the information accessed
- steps had been taken to ensure the nurse in question could no longer access personal health information
- the nurse in question was no longer an employee of the WRHA
- the processes in place (PHIA training, Pledge of Confidentiality) that apply to all WRHA employees including the nurse in question
- their right to contact the WRHA's chief privacy officer and Manitoba Ombudsman with concerns about the breach

[4] Of the 1756 individuals affected, 138 had since died.

On reviewing the WRHA notification letter our office noted that a general description of the breach was provided. Although further details about the type of information accessed (the sort of information maintained in the EDIS system) was not included, the WRHA provided the name and contact information for its chief privacy officer who could be contacted directly with any questions or concerns.

When it was determined following the more comprehensive audit and further analysis that a number of individuals had been specifically targeted (the nurse had searched for their records in EDIS by name), a second notification letter was sent to those individuals on June 12, 2018. This letter explained this new information which had emerged as a result of a deeper analysis of the audit of the nurse's user activity.

Depending on the circumstances of the privacy breach, it may also be appropriate for a trustee that has experienced a breach to also notify others (such as police, insurers, professional and regulatory bodies, technology suppliers and the ombudsman's office). Patients were informed that the College of Registered Nurses of Manitoba and the ombudsman's office had been informed about the unauthorized use of personal health information by the nurse in question. The WRHA notified our office of the results of its investigation on April 26, 2018, and a comprehensive breach report was received by our office on November 7, 2018.

It should be noted that, while individuals have a right of complaint to the ombudsman about the unauthorized use of their personal health information, our office did not receive any complaints from individuals affected by this breach.

Prevention

The fourth step in responding to a privacy breach involves conducting a thorough investigation and evaluation of procedures and safeguards in place at the time of the breach. The purpose is to identify causes and take steps as necessary to develop or improve safeguards to prevent future, similar breaches.

The WRHA noted that the key factor contributing to this breach was that the nurse's status as a casual employee in the Emergency Department at Seven Oaks General Hospital required her to have access to EDIS and this access carried over to her other places of casual employment (for which access to EDIS may not have been required). There is no capacity to refine access to this shared data system by work location (EDIS login credentials are not site specific but system specific). The WRHA explained that it is not practical to temporarily remove and then reinstate EDIS system login credentials from nurses who may work casual days in a number of sites. The WRHA noted, however, that most employees are privacy aware and will not misuse their EDIS system access privileges.

In this case the nurse in question had the requisite privacy training within the last three years (during which the appropriate use of personal health information was explained to her) and had signed a Pledge of Confidentiality. This suggests that it may be appropriate for the WRHA to make modifications to privacy training, such as providing more scenarios dealing with teaching, learning and study situations, which would help employees appropriately apply their authority under the act.

CONCLUSION

Our office determined that the WRHA has adequate policies and procedures in place regarding the security of personal health information under PHIA, including procedures to appropriately address privacy breaches. We have found that the WRHA moved to respond to this privacy breach immediately and it commenced an investigation promptly. Nonetheless, the nurse in question continued to have access to EDIS for three weeks after she was observed acting inappropriately by a co-worker. We recognise that the WRHA considered requesting a removal of the nurse's EDIS access while its internal investigation was ongoing, but concluded that it could not appropriately do so until the full investigation was completed.

We recognize that comprehensive audits of user access must be undertaken to conduct a full investigation and determine the full extent of a breach. However, in cases such as this where the nurse was observed in her inappropriate use by a co-worker, the time of inappropriate access could be determined with certainty. The suspicion of unauthorized use could have been confirmed through an audit of recent access to EDIS enabling a quicker decision about the temporary removal of the nurse's login credentials. Such an approach would strengthen the protection of personal health information and ensure that personal health information is used only for authorized purposes.

It is considered an offence under PHIA for an employee, without the authorization of the trustee, to wilfully use, gain access to or attempt to gain access to another person's personal health information. The ombudsman is permitted to disclose personal health information concerning an offence to the minister of justice and attorney general if the ombudsman has consent from the individual the information is about. As our office did not receive complaints from individuals affected by this breach, we did not have consent to disclose their personal health information for the purpose of pursuing potential charges under PHIA.

October 16, 2020
Manitoba Ombudsman