Report Under the Personal Health Information Act
Case 2017-0143: Winnipeg Regional Health Authority

Privacy Breach Investigation: Use, Disclosure and Security of Personal Health Information Relating to MRI Services

Report issued on April 10, 2019

Manitoba Ombudsman

Table of Contents

This report is available in alternate formats upon request.

Mailing address:	Manitoba Ombudsman 750-500 Portage Avenue, Winnipeg, MB R3C 3X1
Phone:	204-982-9130
Toll-free phone:	1-800-665-0531
Email:	ombudsman@ombudsman.mb.ca

1. INTRODUCTION

This report concerns an investigation initiated by the ombudsman about a privacy violation under the Personal Health Information Act (PHIA or the act). The investigation related to an unauthorized disclosure of the personal health information of 91 patients who received magnetic resonance imaging (MRI) scans within the Winnipeg Regional Health Authority (WRHA or the trustee) between 2008 and 2016. The patients' personal health information was unlawfully disclosed to several media organizations in April 2017.

The personal health information was associated with an audit by the Office of the Auditor General of Manitoba (OAG), titled *Management of MRI Services*, which included an audit of MRI services provided within the WRHA. During the audit, the OAG was given access to patients' personal health information maintained in a diagnostic imaging database. The records that were disclosed to media organizations had been prepared by the OAG based on information maintained in this database. These records were then provided by the OAG to the WRHA during the audit process.

Our office became aware of the unauthorized disclosure to media organizations after the first media story was published on April 17, 2017. The ombudsman subsequently contacted the WRHA and the OAG to obtain information about this privacy breach of patients' information. In view of the seriousness of this privacy breach, the ombudsman initiated an investigation under PHIA and issued a news release[1] advising of our investigation. The WRHA also publicly stated that it was conducting an internal review into this breach.

Some of the patients whose personal health information was unlawfully disclosed learned of this privacy breach when they were contacted by media organizations. The WRHA also directly notified patients affected by the disclosure of their personal health information. Subsequently, our office received privacy complaints from some affected patients. Further to our investigation of these complaints, we provided the complainants with investigation reports in December 2017.

Additionally, we received inquiries from the public and from trustees subject to PHIA. They expressed concern that health information in a format that identifies specific patients was shared during the audit. They also expressed concern that patients were identified by media organizations. In addition, we received questions about what entities the ombudsman can investigate under PHIA. Media organizations and the OAG are not "trustees"[2] under PHIA and our office does not have authority to investigate them. Accordingly, our investigation focused

[1] Please see https://www.ombudsman.mb.ca/news/news/2017-04-19/ombudsman-reviews-privacy-breach.html to view the ombudsman's news release.

[2] Trustees include health professionals, health-care facilities, regional health authorities and all "public bodies" subject to the Freedom of Information and Protection of Privacy Act (FIPPA), such as provincial government departments and agencies, municipal governments and educational bodies.

on the WRHA's handling of the personal health information, as the trustee of the personal health information that was contained in the leaked records.

PHIA regulates how personal health information is to be handled by trustees and prohibits disclosure of personal health information except for purposes authorized under the act. The ombudsman has broad powers of investigation under PHIA, including the power to initiate investigations and to respond to complaints made by individuals under the act.

Our office initiated an investigation of this privacy breach to:

- determine what occurred in the privacy breach incident
- attempt to identify the person(s) who committed the intentional breach (an offence under PHIA)
- review the WRHA's handling of the privacy breach, as the trustee of the personal health information of the affected patients
- identify factors that may have contributed to the privacy breach, including the internal use (sharing) of the breached records within the WRHA and the security safeguards
- identify measures to reduce risks to personal health information and to strengthen privacy practices and compliance with PHIA

In the course of our investigation, we interviewed WRHA employees who were known to have had the records that were subsequently disclosed to media organizations. We also met with and obtained information from OAG staff involved in the audit. Our investigation was not able to determine the identity of the person(s) who made the unauthorized disclosures to media organizations, nor were we able to determine whether the breach originated within the WRHA.

Our office examined the WRHA's use and security of the records that it received from the OAG, which were subsequently unlawfully disclosed to media organizations. The breached records were created as a result of the disclosure of health information in a manner that identified patients. Therefore, it was relevant to consider the WRHA's disclosure to the OAG in light of the requirement under PHIA to limit the amount of personal health information disclosed to that which is necessary to accomplish the purpose.

This investigation report contains our comments on measures that can be taken to strengthen privacy practices and compliance with PHIA. This report is being published due to the seriousness of this privacy breach, the public nature of the breach and the public interest in this matter. This report may also provide learning opportunities for other trustees.

We note that Manitobans entrust their most sensitive and private information, their personal health information, to their health-care providers and the health-care system for the purpose of receiving care. All patients have a right to privacy under PHIA and should be able to expect that their health information will only be shared with health-care providers and others on a need-to-know basis. Health information could reveal a stigmatizing health condition, a

terrifying diagnosis or a "close call," or a health-care journey with an uncertain ending. An unlawful disclosure of personal health information not only erodes public trust, it takes away patients' control over with whom they wish to share their information, the extent of the information that patients wish to share and when they choose to share it.

The intentional violation of patients' privacy through an unauthorized disclosure of personal health information is a deeply concerning matter. It is also a serious matter under PHIA because it constitutes an offence, for which the offending person may be subject to prosecution and, if found guilty, may be liable for a fine of up to $50,000. The timeframe in which a prosecution may be commenced is within two years from the offence, and therefore in this case, the timeframe expires in April 2019.

2. LEGISLATIVE FRAMEWORK FOR THE INVESTIGATION

The Personal Health Information Act (PHIA) came into effect in December 1997. One of the purposes of this law is to establish rules that regulate the handling of personal health information in a manner that recognizes individuals' right to privacy of their personal health information (section 2 of PHIA[3]).

The ombudsman upholds privacy and access to information rights of individuals under PHIA. Individuals have a right to make a privacy or an access to information complaint to the ombudsman about their personal health information. For example, a privacy complaint may be about a collection, use or disclosure of personal health information by a trustee or a failure to protect the information in a secure manner (subsection 39(2) of PHIA). The ombudsman also has the power to initiate complaints, investigations and audits about a trustee's compliance with PHIA. In addition to investigating the privacy complaints we received from individuals about the disclosure of information related to their MRI scans, our office initiated a broader investigation of the privacy breach and the WRHA's response to the breach (clause 28(a) of PHIA).

PHIA applies to personal health information, which means recorded information about an identifiable individual that relates to:

- the individual's health, or health-care history, including genetic information
- the provision of health care to the individual, or the payment for health care provided to the individual
- the personal health identification number (PHIN) and any other identifying number or symbol assigned to an individual
- any identifying information about the individual that is collected in the course of, and is incidental to, the provision of health care or payment for health care

[3] The appendix contains legislative provisions.

Health care includes any care, service, or procedure that diagnoses, treats, maintains, or promotes health, prevents disease or injury, or affects the structure or function of the body. Information related to diagnostic tests, such as MRI scans, linked to identifiable individuals is personal health information under PHIA.

PHIA applies to certain people and entities called trustees, which include:

- a health professional, such as a physician, nurse, physiotherapist or optometrist
- a health-care facility, such as a hospital, personal care home, medical clinic or lab
- a health services agency that collects or maintains personal health information
- a public body under the Freedom of Information and Protection of Privacy Act (FIPPA), such as provincial departments and agencies, municipal governments, regional health authorities, school divisions, universities and colleges

The WRHA, as a public body under FIPPA, is also a trustee under PHIA with respect to the personal health information it maintains. The WRHA maintains personal health information about MRI services it provides. Of the three entities involved in this privacy breach, only the WRHA is a trustee under PHIA. Therefore, as the trustee who maintained the personal health information that was subsequently disclosed to the media, the WRHA was the subject of our review. Our review did not determine that the WRHA was responsible for the unauthorized disclosure of personal health information to the media. Nor did it determine that the person(s) responsible for the privacy breach was employed by the WRHA.

The Office of the Auditor General (OAG) is an independent office of the legislature and is not a trustee under PHIA. This is because the definition of a public body under FIPPA specifically excludes "the office of an officer of the Legislative Assembly." As the OAG is not a public body and does not otherwise fall under the definition of a trustee, it is not subject to PHIA. Therefore, our office has no jurisdiction to investigate the OAG.

Media organizations are also not trustees and are not subject to PHIA. Therefore, our office does not have jurisdiction to investigate a media organization's collection, use or disclosure of personal health information. A federal privacy law, the Personal Information Protection and Electronic Documents Act (PIPEDA), applies to private-sector organizations, including those in Manitoba. PIPEDA sets out rules for how private-sector organizations, including media organizations, collect, use or disclose personal information in the course of commercial activities. Compliance with PIPEDA is overseen by the Office of the Privacy Commissioner of Canada. However, the privacy provisions in PIPEDA do not apply when an "organization collects, uses or discloses the information for journalistic, artistic or literary purposes and does not collect, use or disclose for any other purpose."

PHIA sets out restrictions on a trustee's collection, use and disclosure of personal health information. The act prohibits a trustee from using or disclosing personal health information except for purposes authorized under PHIA. Every use and disclosure by a trustee must be for a purpose authorized under PHIA and be limited to the minimum amount of personal health

information necessary to accomplish the authorized purpose. A trustee must also limit its own internal use of personal health information with its employees on a need-to-know basis and limit its disclosure only to the extent that the recipient needs to know the information (sections 20, 21 and 22 of PHIA).

PHIA also requires trustees to protect personal health information by implementing reasonable administrative, technical and physical safeguards that ensure the confidentiality, security, accuracy and integrity of the information (section 18 of PHIA). The Personal Health Information Regulation under PHIA contains additional obligations for trustees with respect to personal health information. For example, a trustee must provide orientation and training to its employees about its written security policy and procedures and ensure that employees sign a pledge of confidentiality (sections 6 and 7 of the regulation).

As noted in the introduction of this report, the deliberate act of using or disclosing personal health information in violation of PHIA is an offence under the act. An employee of a trustee who commits such deliberate acts can be subject to prosecution under PHIA (subsection 63(2) of PHIA). The ombudsman may lay a charge concerning an offence under PHIA. However, the ombudsman cannot disclose identifiable personal health information to the minister of justice and attorney general for the purpose of a prosecution, unless the individual the information is about gives consent for this disclosure (subsection 34(3) of PHIA). This means that individuals who have been affected by a violation of their privacy have the ability to control whether or not their personal health information can be disclosed by our office for the purpose of a prosecution. If the court finds a person guilty of an offence under PHIA, it may impose a fine of up to $50,000 (subsection 64(1) of PHIA).

3. INVESTIGATION

Our investigation examined the privacy breach incident and attempted to identify the person(s) who contravened PHIA by disclosing the personal health information of WRHA patients to media organizations. We considered various possible breach scenarios, including whether someone who received or obtained the records may have leaked them to media organizations or whether someone may have provided the records to a third party or an employee of another trustee who then leaked the records. We reviewed the WRHA's handling of the privacy breach, as it is the trustee of the personal health information of the affected patients. The breached records were created by the OAG during its audit of the management of MRI services and were provided to the WRHA. Accordingly, we met with and obtained information from the OAG.

Through interviews and reviews of documentary evidence, we examined factors that may have contributed to the privacy breach. Our examination included a review of the internal use (sharing) of these records within the WRHA and the WRHA's security safeguards for protecting the personal health information contained in the records. The personal health information involved in the breach had originally been collected by the WRHA in order to provide diagnostic imaging services (health care) to patients. As this information was disclosed to the OAG during

its audit of MRI, we also examined the WRHA's disclosure to the OAG. Although the source of the breach could not be determined, through this investigation we identified measures to reduce risks to personal health information and to strengthen privacy practices and compliance with PHIA.

3.1 Background

On April 6, 2017, the Office of the Auditor General (OAG) publicly released a report of an audit of the Management of MRI Services[4]. The OAG's audit was based mainly on a sample of patient files about MRI scans performed in 2015 at five facilities, which included facilities in the WRHA.[5] A MRI scan is a diagnostic imaging procedure that uses a magnetic field and pulses of radio wave energy to make three-dimensional pictures of organs and structures inside the body. MRI scans can be used to diagnose and monitor medical conditions not seen by normal x-rays, including aneurysms, cancer and brain injuries.

The OAG's report stated that the audit examined the adequacy of processes for ensuring timely and efficient MRI services, and adequacy of processes for ensuring patient safety and the quality of MRI scans and reports. As part of examining processes for ensuring timely and efficient MRI services, the audit examined whether patients were given higher priority for non-medical reasons, including Workers Compensation Board clients, private paying patients, and "patients with influence" (described by the OAG as government officials, donors or people working in the health-care system).[6]

3.2 Discovery of the Privacy Breach

Media organizations began reporting stories on April 17, 2017, that referenced the personal health information of specific individuals. The stories revealed that the personal health information of patients who received MRI services within the WRHA had been unlawfully disclosed ("leaked") to media organizations in contravention of PHIA.

Our office contacted the OAG and the WRHA immediately following the stories reported in the media, as it was evident that a privacy breach had occurred. Both organizations were responsive and cooperative and provided our office with information and documentation relevant to the breach. We also gathered background information regarding the OAG audit of the management of MRI services.

Our initial focus was on identifying the specific personal health information of individuals that was unlawfully disclosed to media organizations. Based on descriptions of the personal health information in media stories, and in consultation with the OAG and the WRHA, we determined that the media appeared to have received three different types of records or parts of records.

---

[4] Office of the Auditor General report on the Management of MRI Services, April 2017

[5] Office of the Auditor General report on the Management of MRI Services, April 2017, page 14

[6] Office of the Auditor General report on the Management of MRI Services, April 2017, page 4

The WRHA and OAG provided us with copies of the records, which had been prepared by the OAG during the audit. The OAG had provided the three records to the WRHA as separate documents on different dates in 2016.

3.3 The Records and Personal Health Information Leaked to Media Organizations

Our office obtained a copy of the records received by media in April 2017. This enabled us to compare the records received by the media with the records that the OAG provided to the WRHA in 2016 that we had previously obtained. Our examination of the records confirmed that the three records matched. However, it appeared that the three different records, which had been sent as separate documents by the OAG to the WRHA on different dates, had been assembled together as a package. This was most likely done by the person(s) who unlawfully disclosed the information. That package was leaked to media organizations. It also appeared that the package had been provided to media organizations in hard copy format.

The following is a description of the three records disclosed to media organizations:

1. "Cover Page"
This is a cover page the Office of the Auditor General's audit plan, titled *Audit Plan, MRI Scan Management*. The cover page was altered by an unknown person who removed the date on the cover page.

We determined that the cover page disclosed to media organizations was almost identical to the cover page of two audit plans prepared by the OAG and provided to the WRHA and the other auditees in the early stages of the OAG's audit of MRI services. In preparation for the audit, the OAG provided a draft audit plan to auditees in January 2016. The OAG also provided auditees with a final audit plan dated March 2016. However, as the date was removed from the cover page before it was provided to media organizations, we could not determine from which plan the cover page originated. This record contained no personal health information.

2. "Table"
This is a one-page table prepared by the Office of the Auditor General titled, *WRHA PREFERENTIAL TREATMENT FINDINGS.* This table does not include the names of patients. The table contained the following three columns of information:

- Category: This column listed six categories of "influence" that patients were said to belong (board member, donor, politician, professional sports player, radiologist, senior management of WRHA)
- Number of people with MRI: This column provided the numbers of patients within each category who received MRI scans
- Number of instances of potential preferential treatment: This column identified the number of instances of potential preferential treatment related to MRI scans identified by the OAG that were provided to the patients in the particular category

This table was identical to a table of data prepared by the OAG and provided to the WRHA in July 2016. Although patients are not named in the table, some may be identifiable given the small number of people who could potentially fall within the categories being examined in this aspect of the audit.

This table was originally sent by the OAG to the WRHA in the course of providing information relating to preliminary findings of the audit. Prior to receiving this table, the WRHA had received more general information from the OAG with respect to this aspect of the audit. The WRHA requested further information from the OAG regarding the OAG's analysis of the "persons of influence" in order for the WRHA to review and respond to issues raised by the OAG's preliminary findings. In response, the OAG sent the table to two WRHA employees as an attachment to an email in July 2016.

3. "List"

This is a five-page list prepared by the Office of the Auditor General titled, *Audit Details – WRHA, Confidential*. It is a list that contains personal health information of 91 patients. The list contains five columns of information about the patients:

- first name
- last name
- category (meaning the category of influence as defined above by the OAG)
- exam date
- facility (the name of the facility within the WRHA)

The list does not specifically reference the OAG or MRIs. The list contains the personal health information of 91 named patients; however, as some patients on the list had more than one "exam date" the number of exams added up to 190. The exam dates ranged between 2008 and 2016.

Further to the WRHA receiving preliminary audit findings and the table from the OAG in July 2016, the WRHA asked the OAG in August 2016 to send it patient numbers in order for the WRHA to review the timelines for the MRI scans the patients received. The OAG explained to our office that it needed to use patient names in its testing for preferential treatment, and therefore patient numbers were not recorded in their working papers. The OAG advised that, because the request for further information regarding potential preferential treatment came from the trustee of the information, the OAG sent the list containing the names of 91 patients, their category (as defined by the OAG), their exam date(s) and facility name, to two WRHA employees in September 2016.

The list was an excel spreadsheet that was password protected and attached to an email. The personal health information contained in the list was information sourced from the WRHA's diagnostic imaging database, which was made available to the OAG during the MRI audit. Our

office was able to confirm that the list the OAG sent to the WRHA in September 2016 was identical to the list received by media organizations.

We note that media organizations referred to the leaked records as being a "confidential report" from the Office of the Auditor General. We observed that all three records, though created by the OAG at different points in time and provided to the WRHA at different points in time, had been assembled as a package. It is unclear whether the person(s) who disclosed the records intended to portray the records as comprising a confidential report of the OAG. Although the date on the cover page of the OAG's audit plan had been removed, it clearly was identified as being from the OAG's audit plan. However, the other two records were not part of the audit plan documents and were not in existence when the audit plans were created.

We considered that the list of names did not indicate that the personal health information was related to the OAG or MRI scans, nor did it allege potential preferential treatment. Had the list been the *only* record disclosed to media organizations, we observe that this record would not be as readily associated with the OAG's audit of the management of MRI services. The cover page of the OAG's audit plan would therefore connect the list to the OAG's audit of the WRHA's MRI services. The table titled *WRHA PREFERENTIAL TREATMENT FINDINGS* did not include patients' names or mention the OAG. However, the combination of these three records appears to intentionally portray those named in the list as being found by the OAG to have received preferential access to MRI scans.

We also considered the timing of the disclosure to media organizations. We note that the records involved in the privacy breach had been provided by the OAG to the WRHA several months prior to the leak to media organizations. The OAG's audit had been released publicly on April 6, 2017. The WRHA was first contacted by the media about the leaked records on Monday, April 17, 2017. It would seem likely that when the records were received by media organizations, this would have prompted the contact with the WRHA. The first article was posted on a media organization's website at 8 p.m. on April 17, 2017. We noted that other media organizations reported on the issue on April 18, 2017. Based on information and reasonable assumptions, we believe that the unauthorized disclosure to media organizations occurred on or around Monday, April 17, 2017.

3.4 Review of the WRHA's Response to the Privacy Breach

When a privacy breach occurs, our office expects trustees to take swift action in response. To assist trustees, our office has published a practice note titled *Key Steps in Responding to Privacy Breaches*[7]. This guidance document outlines four key steps: containing the breach, evaluating the risks associated with the breach, notifying affected individuals and preventing a reoccurrence.

[7] https://www.ombudsman.mb.ca/uploads/document/files/practice-note-keys-steps-in-responding-to-privacy-breaches-2018-en.pdf

We reviewed the WRHA's response to the unauthorized disclosure of WRHA patients' personal health information to media organizations. The WRHA learned of the privacy breach when it was contacted by the media on April 17, 2017. We note that immediately after the WRHA learned of the breach it was necessary for the WRHA to determine the specific health information involved and identify which individuals were affected by the breach. While it became apparent that the breach involved personal health information of patients who had MRIs at the WRHA, it was not immediately known by the WRHA what records had been given to media organizations.

The WRHA has a policy and corresponding procedures on reporting and investigating privacy breaches. On April 18, 2017, the day following the first media story, the WRHA notified our office that it would commence an internal investigation of the disclosure of personal health information to the media. On that same day, a message was sent to WRHA staff advising of the breach, and informing staff that the WRHA would commence an internal investigation.

Responding to a privacy breach is often time and labour-intensive. It is important that a trustee undertake a careful assessment to accurately identify the individuals and the specific personal health information about them involved in the breach. Misidentification of individuals or the information about them can create unnecessary stress for the individuals. A trustee's decision about notifying individuals should be based on an evaluation of the risks associated with the breach.

A relevant consideration was that this breach involved an intentional leak of personal health information to, and reporting on by, media organizations. We acknowledge that the period following the media stories about the leaked personal health information would have caused significant stress for many patients, including people who were not on the list. People who were advised by media they were on the list, and other people who may not have been on the list, may have felt forced to have conversations about a diagnosis or treatment they received at a particularly difficult time in their lives. As this breach would have potentially left many patients wondering if their personal health information was disclosed, the WRHA determined that it was important to notify all patients whose personal health information had been unlawfully disclosed to media organizations.

Determining the personal health information involved in this breach and identifying the specific affected individuals based on descriptions in media stories posed challenges for the WRHA. The WRHA proceeded in a timely manner to identify potential affected individuals based on the likelihood that the media had received the list of patients that the OAG had prepared and provided to the WRHA in September 2016. This was a reasonable conclusion based on the information available to the WRHA, which was later confirmed when our office obtained and compared a copy of the records received by media. Another significant factor in notifying the affected individuals was verifying their current contact information. The 91 patients on the list had exam dates ranging between 2008 and 2016. Given that some of these scans were performed nine years prior to the breach, it was possible that patients may have moved or died

during this period. Therefore, the WRHA had to ensure it had accurate contact information for the individuals.

The WRHA prepared notification letters to patients affected by the breach and sent them within days of the trustee determining the scope of the privacy breach. On April 27, 2017, the WRHA completed notification to individuals affected by the breach. The notification letters to the affected patients included a description of the breach, a description of the information disclosed, and notification that the WRHA was conducting an investigation into the breach. The letters also contained the contact information of the WRHA's chief privacy officer should the patient have additional questions or concerns, as well as information on how to contact or make a complaint to the ombudsman.

Based on our review of the WRHA's response to the privacy breach, we believe that it acted as quickly as possible in the circumstances to identify and notify affected individuals. The WRHA's notification letters provided the victims of the breach with relevant details and appropriate contact information both for the chief privacy officer as well as for our office.

The WRHA also conducted an in-depth internal review of the breach and provided a copy of its report to our office. The internal review confirmed who within the WRHA had a copy of each record that had been provided to media organizations, if/how each record was shared internally by WRHA staff, and how each record involved in the breach had been stored by WRHA staff. The WRHA's review determined the staff within the WRHA who had access to all three records that were disclosed. The review was not able to identify any evidence that the records, including the list of patients, had been disclosed by someone from the WRHA to anyone, including to media organizations.

3.5 WRHA's Use of Personal Health Information that was Subsequently Involved in the Breach

The three records disclosed to media organizations in 2017 were created by the OAG during its audit and were provided by the OAG to the WRHA at different points in time in 2016. Our investigation traced the pathway that the records, particularly the list of patients, travelled within the WRHA. Using the WRHA's internal review as an initial reference point, we identified WRHA employees who were known to have had contact with all three records, including the list of patients. We considered when, how and why the employees had these records. To examine the WRHA's handling of the records, we conducted our own interviews of WRHA employees.

The purpose of the interviews was to examine each employee's use (for example, sharing) of the personal health information, as well as to examine the measures taken to safeguard the personal health information while it was in the employee's possession. These interviews were important in trying to identify the person(s) involved in the breach incident. The interviews also provided information relevant to our assessment of the WRHA's compliance with the requirements of PHIA. In particular, we gathered information with respect to limiting the use of

personal health information to those employees who need to know it to perform their job duties and limiting the amount of personal health information used by those employees to only that which was required for the purpose for which the information was used.

We identified that nine employees within the WRHA were known to have had a copy of the OAG's list of patients (or a partial copy of the list) in their possession at some point prior to the breach incident in April 2017. We conducted interviews of all employees who were known to have had a complete or partial copy of the list, including current and former employees of the WRHA. The people interviewed ranged in role from senior executives to employees involved in the WRHA's review of the OAG's data regarding the "persons of influence." As our investigation did not find any evidence that the people we interviewed were involved in the breach incident, we are not identifying them as doing so could unfairly damage their reputations.

Our interviews were tailored to the employee's role, but generally included the following:

- their role in the OAG audit of MRI services
- their use of electronic and hard copies of the list, including whether they shared the list with anyone
- their storage of the list, including measures taken to safeguard the personal health information it contained
- their awareness of anyone else who may have had a copy of the list
- their knowledge of anyone who had a motivation to disclose the records

Employees within the WRHA's diagnostic imaging program had direct involvement in the OAG's audit of MRI services. The OAG provided the list by email to its two main contacts who worked in the WRHA's diagnostic imaging program on September 6, 2016. This email by the OAG followed a request by the WRHA for a list of patient numbers corresponding to the "persons of influence" data in the table that had previously been provided by the OAG in July 2016.

The WRHA stated that it requested this information from the OAG so that it could conduct its own review of the data. The WRHA advised that its request to the OAG for patient numbers referred to accession numbers. Accession numbers uniquely identify each patient's scan and having these accession numbers would enable the WRHA to perform searches within the diagnostic imaging database in order to review the data about the scans. The WRHA received the list of patient names and other details instead of the accession numbers corresponding to the scans of the "persons of influence." As noted earlier in this report, the OAG recorded their data by the name of the patient and did not have accession numbers.

Three copies of the list were printed and a hard copy was subsequently shared with an employee in senior management within the diagnostic imaging program. Additionally, a hard copy of the list was shared with a program manager in order that two staff could review the OAG's data related to the list of 91 patients who were purported to have received preferential treatment. The manager physically divided a hard copy of the list in two and provided the half copies of the list to two staff for review. Given the role of the program staff in reviewing the

information contained in the list and comparing it with the information contained in the database, it was necessary for them to have full access to the personal health information contained in the list. Within approximately two days, the list with notations made by staff was subsequently returned to the WRHA's main contact for the audit who retained the annotated hard copies of the list until approximately October 2016.

The WRHA's audit services was also asked to review the OAG's results, and received a photocopy of the list and also gathered the hard copy lists and records from the WRHA's main contact for the audit. The employee in senior management noted above provided his hard copy of the list to a WRHA senior executive. Finally, a photocopy of the list was also provided to another senior employee who worked closely with the senior executive.

As stated above, the list was received from the OAG in order for the WRHA to conduct its own assessment of the data. With respect to the use of the personal health information, it is important to consider whether the information is shared only with those who need to know the information. It is also important to consider whether the sharing of that information is limited to the minimum amount of information needed to accomplish the purpose. We determined that relevant employees and management were informed of the OAG's preliminary audit findings and issues identified about potential persons of influence. However, we also observed that of the nine WRHA staff who received a copy of the list, the only staff who might have needed to know the identities of all of the specific patients contained in the list were the staff that had responsibility to assess the OAG's preliminary findings. For WRHA staff who received the list but did not need to know the patient names, we believe that the WRHA could have provided those staff with a redacted version of the list that did not include names of patients. Taking this action would have further limited the amount of personal health information shared within the WRHA.

In order to reduce the risk of a privacy breach, it is important for trustees to carefully consider ways to limit the amount of personal health information shared. One way to potentially mitigate risk is to de-identify personal health information when identifiable information is not required for the purpose of the use of the personal health information.

3.6 WRHA's Security of Personal Health Information that was Subsequently Involved in the Breach

Our investigation also considered the steps taken by the WRHA to safeguard the personal health information contained in the list. PHIA requires trustees to implement reasonable administrative, technical and physical safeguards that ensure the confidentiality, security, accuracy and integrity of personal health information. This requirement applies to electronic, as well as physical, records. In our investigation, as well as in the WRHA's internal review, the electronic handling of the list was examined.

The list had been sent by the OAG as an attachment to an email to two WRHA employees. The attached list was password protected. The password for the list was sent in a separate email by the OAG to the WRHA employees. The emails received by the WRHA employees were stored in the employees' email inboxes, to which no other staff had access. There was no evidence that the list had been forwarded electronically. One employee saved the list on their network drive that requires a password to enter. The list itself remained password protected on the network drive, requiring two passwords to access it – one for the network and one for the list.

An issue that emerged during our interviews with WRHA staff was that although the list was shared with few people within the WRHA, the hard copies were not secured in locked storage when not being used by staff (in locked cabinets or locked offices). In one instance, the file cabinet where the list was stored was not lockable and the employee's office also could not be locked. Although the door to the general office area would be locked after work hours, anyone who accessed the general office could potentially access the employee's office during the approximately one month period it was stored in this location.

The office doors for program staff of the WRHA's diagnostic imaging program were not locked during the day if staff were present. Locks on the doors in the diagnostic imaging offices were in the process of being replaced with swipe card access. However, the door to central intake for the diagnostic imaging office had not yet been modified for swipe card access at the time when the list was stored there for approximately two days. A copy of the list was not always in locked storage for approximately one week in another office. In only one instance was a copy of the list stored in a consistently locked file cabinet when the record was not being used.

In this case, physical safeguards for the hard copies of the list that were available were not reasonably employed at all times when the list was stored by staff. Sensitive information should be kept in locking file cabinets, for example, when the information is left unattended for a period such as when an employee leaves for the day, or if a program area is accessible to others. As well, doors to program areas should provide secure access to only those who are required to be in the area, given that personal health information is handled on a daily basis by staff.

Despite the weaknesses in physical safeguarding of the list, there were very few instances where the other two breached records were stored with the list. When all three records were stored together, anyone seeking access would need to have known the records were there and where the records were filed within a cabinet of files, or undertake a search of the cabinet for the records.

There was no evidence that individuals exploited these weaknesses in security to obtain the records for the purpose of leaking them. Although these safeguards may not have altered the outcome in this case, ensuring that personal health information is stored securely serves to protect the privacy of the information contained in the records and helps to prevent accidental or intentional privacy breaches.

3.7 WRHA's Disclosure of Personal Health Information to the OAG during the Audit of MRI Services

The personal health information contained in the records leaked to media organizations had originally been collected by the WRHA in order to provide diagnostic imaging services (health care) to patients. During the OAG's audit of the management of MRI services, the WRHA disclosed health information about identifiable patients (personal health information) to the OAG. PHIA permits a disclosure for a purpose authorized under the act if the disclosure is limited to the minimum amount of personal health information necessary to accomplish the authorized purpose. The disclosure must also be limited to the extent that the recipient needs to know the information.

To help us understand the disclosure of personal health information by the WRHA to the OAG, we reviewed information about the scope of the OAG's audit. Our review included both the draft and final audit plans that the OAG provided to the WRHA in January and March 2016 respectively, as well as the audit report released publicly in April 2017. We also interviewed WRHA staff who were involved in the audit, as well as staff who facilitated the disclosure of personal health information to the OAG.

The WRHA disclosed personal health information to the OAG by providing auditors with direct access to its diagnostic imaging database. At the time of the audit, the database included patient files for MRI scans performed between 2008 and 2016, which amounted to approximately 470,000 MRI scans. The database also contained personal health information about a variety of other diagnostic imaging services performed, including ultrasound images, x-rays, positron emission tomography (PET) scans, digital mammography, pathology scans, and dental scans.

With respect to the personal health information related to these various diagnostic imaging procedures, a patient's file could also include any associated bloodwork, radiology reports, notations regarding any additional concerns with the patient, the patient's personal health identification number (PHIN), demographic information, and a pre-screening form related to a diagnostic image. For example, the form that requests consultation for a diagnostic imaging exam (including MRIs) captures information about the patient's history and provisional diagnosis, whether the patient is pregnant, their maiden name, their emergency contact/next of kin and whether the patient has various other conditions (such as having implanted devices, claustrophobia or sleep apnea).

The OAG's public audit report indicated that the audit at five facilities (which included facilities in the WRHA) was "primarily based on a random selection of 270 outpatient and 85 inpatient files from the population of MRI scans performed in 2015 (with additional patient files selected in specific areas as needed)."[8] With respect to only the facilities in the WRHA, the final audit

[8] Office of the Auditor General report, April 2017, page 14

plan indicated that the OAG would be reviewing 210 outpatient files from the calendar year 2015, 40 inpatient files, and 30 third-party payer files (MRI scans paid for by a third party).

The OAG included audit testing to examine whether "patients with influence" received expedited access to MRI scans as a part of examining whether MRI requests are scheduled efficiently and in a timely manner according to priority level. OAG staff advised our office that this testing was discussed with key WRHA personnel involved with the audit at the audit plan meeting. The OAG described this testing in a bullet point in schedule 2 of the audit plans as "investigate jumping the queue scenarios." A date range was not specified for this test.

From our review of the OAG's list of 91 individuals that was disclosed to the media, the OAG's access to personal health information in the diagnostic imaging database extended as far back as 2008 and up to 2016. For the purposes of investigating jumping the queue scenarios, the OAG advised our office that within the WRHA's diagnostic imaging database, it searched the names of hundreds of people who it identified as fitting within the categories of influence being probed. Specifically, the OAG advised that their process was as follows:

- they determined the categories of persons of influence to test
- they developed a list of names of individuals under each category to test
- they searched each name on the list in the database to determine whether they had received an MRI
- they determined when the MRI was requested (based on the requisition), how it was prioritized (if applicable) and when the related scan was received

Based on our interviews of WRHA staff and our examination of their internal correspondence, it was apparent that the WRHA staff directly involved in the audit were surprised that the personal health information of individuals from 2008 to 2016 was accessed in order to investigate jumping the queue scenarios. Although the WRHA provided the OAG with access to its entire diagnostic imaging database as discussed above, WRHA staff believed that the audit tests were being performed within the sample of patient files from 2015 until they received the preliminary audit findings and the list that included patients who received scans between 2008 and 2016. We note that the trustee is ultimately responsible under PHIA for its disclosure. Accordingly, it is essential for a trustee to ensure that it has a clear understanding of the personal health information it is disclosing in an audit (for example, files within certain date ranges).

Access to the diagnostic imaging database is electronically logged and is auditable to determine who accessed personal health information and ensure access is for an authorized purpose. PHIA requires trustees to conduct audits of user activity for detecting unauthorized access to personal health information. Additionally, patients are entitled to request a record of user activity showing who accessed their health information. The WRHA provided the OAG staff with unique user identifiers, which enables the WRHA to identify access by the OAG staff within a record of user activity. We note that a trustee's own audit of user activity, or a patient's request for a record of user activity, can occur years after the patient's records were accessed. It would

be difficult for a trustee to explain the access to patient files if a trustee is not aware of the fact that the personal health information was within the scope of information to be accessed during an external audit (for example, when the access does not appear to match the date range of the files that staff believed were included in an audit).

To ensure compliance with PHIA and accountability to individuals, a trustee must be able to demonstrate that its disclosure meets the requirements under PHIA. With respect to a disclosure to the OAG, we note that FIPPA contains a specific authorization for disclosure of personal information to the Auditor General (clause 44(1)(h) of FIPPA). PHIA does not contain the same or similar authorization for a disclosure of personal health information. However, both FIPPA and PHIA (clause 22(2)(o) of PHIA) authorize disclosure if another act permits or requires the disclosure, which would include the Auditor General Act. We observe that the Auditor General Act provides authority to the OAG to access records of any government organization that are necessary for the purpose of that act (section 18 of the Auditor General Act).

A trustee's disclosure that is authorized under another act, including the Auditor General Act, is not incompatible with PHIA. Section 18 of the Auditor General Act provides authority to the OAG to determine the scope of an audit and the information necessary for the audit. PHIA requires the trustee to limit the disclosure to the minimum amount of personal health information necessary for the OAG's purpose under the Auditor General Act (subsection 20(2) of PHIA) and disclose only to the extent that the recipient (OAG) needs to know that personal health information (subsection 22(3) of PHIA). This does not imply that the trustee determines what information the OAG requires for an audit. It does however require a trustee to determine that its disclosure complies with PHIA. This means that a trustee must ensure that it has a clear understanding of the OAG's scope of the audit, and the personal health information required for the audit.

The requirement in PHIA to limit the disclosure of personal health information to the "minimum amount of information necessary to accomplish the purpose" requires a thorough assessment of the specific information that is required in each situation. An assessment should include considerations about:

- whether the purpose for the disclosure can be accomplished with less health information about individuals
- whether the health information needs to linked to identifiable individuals to accomplish the purpose
- whether measures can be taken to limit the disclosure to that which is necessary if the necessary elements of personal health information are intermingled with unnecessary information

To ensure a clear understanding of the personal health information needed and in order to facilitate a disclosure that complies with the requirement to limit the amount of information to

that which is needed, the assessment requires clear communication between the trustee and the OAG.

4. STRENGTHENING PRIVACY PRACTICES AND COMPLIANCE WITH PHIA

As we were not able to determine the manner in which the individual(s) responsible for the privacy breach obtained the personal health information that was disclosed to media organizations, we were not able to identify specific measures that would have been prevented this breach. However, our investigation identified ways in which trustees can minimize the risks to personal health information when it is being used and disclosed. This includes circumstances where the information relates to a large number of patients, such as in the case of making bulk disclosures. The following considerations are provided to assist trustees in strengthening privacy practices and compliance with PHIA.

Engage the Privacy Officer in Decisions about Bulk Disclosures of Personal Health Information

Bulk disclosures and/or highly sensitive information and/or disclosures made to non-trustees should be carefully considered by a trustee. Trustees that are larger institutions generally have experience with respect to such disclosures in the context of making disclosures to researchers. Such disclosures should engage relevant staff to ensure that privacy of individuals remains a paramount consideration. When bulk disclosures are made in the context of an external audit, trustees should engage their organization's privacy officer in the audit, as this employee has expertise in, and general responsibility for, facilitating the trustee's compliance with PHIA.

Determine the Specific Elements of Information Required

Collecting, maintaining, using and disclosing personal health information creates risk for a breach of privacy to occur, whether inadvertently or intentionally. The requirements of PHIA to limit collection, use and disclosure of personal health information, and the requirements to implement security safeguards to protect the information, serve to mitigate the risks of breaching individuals' privacy. Generally, the privacy risks increase as the amount of personal health information increases, as the level of sensitivity of the information increases and as the information more readily identifies individuals the information is about.

When the purpose for collecting, using or disclosing personal health information is to provide health care or another service directly to the individual, the information would reasonably need to readily identify the individual (for example, patient name, PHIN, etc.). However, PHIA expressly recognizes that persons other than health professionals now obtain, use and disclose personal health information in different contexts and for other purposes. This also can contribute to privacy risks, which need to be assessed and mitigated.

PHIA sets out requirements relating to disclosures for the purpose of research, which generally involve the personal health information of a large number of individuals (bulk disclosures). The following suggestions relate to bulk disclosures for other purposes, including audits.

To ensure compliance with PHIA and to reduce the risk of privacy breaches, discuss, develop and document a plan for a bulk disclosure to ensure that the trustee and the recipient of the information have carefully considered and clearly understand the following:

- what specific elements of information are required
- whether it is necessary to disclose personal health information that identifies specific patients or whether the elements of health information required can be disclosed without disclosing the identities of patients
- if health information needs to linked to identifiable individuals, consider the least privacy-invasive identifiers and only use names if necessary (for example, using an accession number that identifies a specific MRI scan of a particular individual is less privacy invasive than using the individual's name because someone would need to have access to the database to search the accession number in order to identify the individual who had the scan)
- what measures can be taken to limit the disclosure to the amount of personal health information required for the purpose of the audit and to the extent that the recipient needs to know the information
- if personal health information about identifiable individuals needs to be disclosed to the recipient, consider whether the recipient needs to retain it in an identifiable form and consider whether measures can be taken at the earliest opportunity to de-identify or remove information that allows individuals to be more readily identified (for example, consider options to minimize the personally identifying information by using other identifiers (such as patient number, etc.) or by using accession numbers instead of names)

Implement Reasonable Security Safeguards

PHIA requires trustees to adopt reasonable administrative, technical and physical safeguards for personal health information. This includes practical measures, such as ensuring that lockable file cabinets and doors are available to and used by all staff handling sensitive personal health information. If an atypical situation arises, such as one involving particularly sensitive personal health information, determine whether to implement specific measures for special handling the information involved. For example, create a watermark across printed records to uniquely identify each copy and then track to whom each copy is provided and when.

Ensure the Amount of Personal Health Information Used is Limited and Based on the Need to Know

For each use (sharing) of records between employees of a trustee, determine whether the other employee needs to know the personal health information. Consider whether it is possible

to minimize/redact or de-identify personal health information when sharing records amongst staff, if the identities of patients are not required for the purpose of providing the records.

Ensure Mechanisms are in Place for Accountability to Individuals

Individuals have a right under PHIA to request a copy of a record of user activity to see who accessed their personal health information. In this case, the OAG auditors who accessed the digital imaging database were issued unique user identification and this would enable access to be logged and electronically auditable. As the trustee is responsible under PHIA for the disclosure of personal health information, it is important to have a clear understanding of and documentation about the scope of the disclosure. This will enable a trustee to answer questions about a record of user activity and be accountable to individuals for the disclosure of their personal health information.

5. CONCLUSION

PHIA exists to protect the personal health information of all Manitobans. Under PHIA, there is no sliding scale for privacy and the law does not differentiate who should have more, or less, privacy under PHIA. It is irrelevant under the law whether you may be a prominent citizen, such as someone who might be considered a person of any potential influence. A deliberate decision to violate PHIA could potentially expose any Manitoban to the risk of having their personal health information illegally accessed or disclosed publicly in some manner based on someone else's judgement that their neighbour, relative, former partner or friend, co-worker or even a public figure, including media, is not deserving of privacy.

The decision to disclose personal health information must be based on lawful, authorized purposes under PHIA. In this case, there was a deliberate decision to disregard the requirements of PHIA through the unauthorized disclosure of personal health information of 91 patients.

Although our investigation was not able to determine who provided the personal health information to media organizations, our review has identified several measures that trustees should consider in an effort to minimize the risk of intentional or inadvertent privacy breaches in the case of bulk disclosures of personal health information.

Manitoba Ombudsman
April 10, 2019

APPENDIX

Relevant Provisions of the Personal Health Information Act (PHIA)

"personal health information" means recorded information about an identifiable individual that relates to

(a) the individual's health, or health care history, including genetic information about the individual,

(b) the provision of health care to the individual, or

(c) payment for health care provided to the individual, and includes

(d) the PHIN and any other identifying number, symbol or particular assigned to an individual, and

(e) any identifying information about the individual that is collected in the course of, and is incidental to, the provision of health care or payment for health care;

"trustee" means a health professional, health care facility, public body, or health services agency that collects or maintains personal health information.

"public body" means a public body as defined in The Freedom of Information and Protection of Privacy Act, and for the purpose of this definition, the definitions of "department", "educational body", "government agency", ''health care body", "local government body" and "local public body" in that Act apply;

Purposes of this Act

2 The purposes of this Act are

(a) to provide individuals with a right to examine and receive a copy of personal health information about themselves maintained by a trustee, subject to the limited and specific exceptions set out in this Act;

(b) to provide individuals with a right to request corrections to personal health information about themselves maintained by a trustee;

(c) to establish rules governing the collection, use, disclosure, retention and destruction of personal health information in a manner that recognizes

(i) the right of individuals to privacy of their personal health information, and

(ii) the need for health professionals to collect, use and disclose personal health information in order to provide health care to individuals;

(d) to control the collection, use and disclosure of an individual's PHIN; and

(e) to provide for an independent review of the decisions of trustees under this Act.

Duty to adopt security safeguards

18(1) In accordance with any requirements of the regulations, a trustee shall protect personal health information by adopting reasonable administrative, technical and physical safeguards that ensure the confidentiality, security, accuracy and integrity of the information.

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.

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.

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….

Disclosure without individual's consent
22(2) A trustee may disclose personal health information without the consent of the individual the information is about if the disclosure is

(o) authorized or required by an enactment of Manitoba or Canada.

Limit on disclosure
22(3) A trustee may disclose information under subsection (2), (2.1) or (2.2) only to the extent the recipient needs to know the information.

General powers and duties
28 In addition to the Ombudsman's powers and duties under Part 5 respecting complaints, the Ombudsman may

(a) conduct investigations and audits and make recommendations to monitor and ensure compliance with this Act;

Information about offences
34(3) The Ombudsman may disclose to the Minister of Justice and Attorney General information relating to the commission of an offence under this or any other enactment of Manitoba or Canada if the Ombudsman considers there is reason to believe an offence has been committed, except that personal health information must not be disclosed without the consent of the individual the information is about.

Right to make a complaint about privacy
39(2) An individual may make a complaint to the Ombudsman alleging that a trustee

(a) has collected, used or disclosed his or her personal health information contrary to this Act; or
(b) has failed to protect his or her personal health information in a secure manner as required by this Act.

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

(a) discloses personal health information in circumstances where the trustee, Information manager or health research organization would not be permitted to disclose the information under this Act; or
(b) uses, gains access to or attempts to gain access to another person's personal health information;

is guilty of an offence.

Prosecution within two years
63(6) A prosecution under this Act may be commenced not later than two years after the commission of the alleged offence.

Penalty
64(1) A person who is guilty of an offence under section 63 is liable on summary conviction to a fine of not more than $50,000.

Relevant provisions of the Personal Health Information Regulation under PHIA

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.

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.

Relevant Provision of the Freedom of Information and Protection of Privacy Act (FIPPA)

Disclosure of personal information
44(1) A public body may disclose personal information only
(h) to the Auditor General or any other person or body for audit purposes;

Relevant Provisions of the Auditor General Act

Access to records

18(1) Despite any other Act, the Auditor General is entitled to access at all reasonable times to the records of any government organization that are necessary for the purpose of this Act.

Access to information

18(2) The Auditor General may require and is entitled to receive any information necessary for the purpose of this Act from

(a) any person in the public service or formerly in the public service;

(b) any current or former director, officer, employee or agent of a government organization or of a recipient of public money; or

(c) any other person, organization or other body that the Auditor General believes on reasonable grounds may have information relevant to an examination or audit under this Act.

Relevant provision of the Personal Information Protection and Electronic Documents Act (PIPEDA)

Clause 2(c) of Part 1 of PIPEDA reads as follows:

Limit

(2) This Part does not apply to

(c) any organization in respect of personal information that the organization collects, uses or discloses for journalistic, artistic or literary purposes and does not collect, use or disclose for any other purpose.