Manitoba Ombudsman

REPORT UNDER
THE PERSONAL HEALTH INFORMATION ACT

CASE 2014-0500

MANITOBA HEALTH, SENIORS AND ACTIVE LIVING
PROVINCIAL DRUG PROGRAM

PRIVACY INVESTIGATION: COLLECTION, USE, DISCLOSURE, SECURITY

REPORT ISSUED ON DECEMBER 7, 2017

TABLE OF CONTENTS

INTRODUCTION

This report concerns an investigation initiated by the ombudsman under the Personal Health Information Act (PHIA), relating to incidents of an employee's unauthorized access to the personal health information of several individuals in the databases of the Provincial Drug Program (PDP) branch within Manitoba Health, Seniors and Active Living (MHSAL, the department or the trustee). The department notified our office of the privacy breach in October 2014. At that time, the department was conducting its own investigation to determine the extent of the breach. After the department notified affected individuals about the breach, several of those individuals made privacy complaints to our office.

Accessing personal health information for non-work related purposes is not an authorized use of that information under PHIA and is contrary to the act. PHIA was amended on December 5, 2013 to make it an offence, under clause 63(2)(b) of PHIA, for an employee of a trustee (such as the department) to wilfully use, gain access to, or attempt to gain access to another person's personal health information, contrary to the act. This amendment was requested by our office as a result of an investigation of a previous snooping incident related to another trustee.

While not all privacy breach reports to our office result in a formal investigation, in this case we felt the particular circumstances warranted an independent review. Our review of this breach and the individual privacy complaints found that the majority of unauthorized accesses by the MHSAL employee took place before such access became an offence under PHIA. We identified some instances of unauthorized access that occurred between December 5, 2013 and the end of June 2014, when the employee ceased to have access to personal health information.

PHIA permits the ombudsman to disclose information to the minister of justice and attorney general (the Crown), if the ombudsman has reason to believe that an offence has been committed under the act. However, personal health information may only be disclosed by our office if we have the consent of the individual the information is about. One individual consented to the disclosure of their personal health information for this purpose, which resulted in the Crown authorizing the ombudsman, in April 2016, to charge the employee with an offence under clause 63(2)(b) of PHIA. At the suggestion of the Crown, our office deferred completion and issuance of this investigation report pending the prosecution.

On May 31, 2017, a trial was held in this matter and the employee was found guilty of committing an offence by using or accessing the personal health information of the individual contrary to the requirements of PHIA. On September 22, 2017, the court issued a written decision and the employee was sentenced to a fine of $7,500.

In addition to examining the incidents of unauthorized access by the employee, our investigation examined the department's response to these incidents, including the measures in place to prevent, detect and respond to unauthorized access.

We found that the department failed to respond in a timely way to the incidents of unauthorized access by one of its employees and that the department did not, at the time, have in place sufficient policies, procedures and other safeguards to meet its obligations under PHIA. PDP did

not have adequate role-based access management processes or sufficient processes to detect unauthorized access. It also did not promptly and effectively terminate the employee's access to personal health information once it discovered the unauthorized access.

These deficiencies were not consistent with the department's obligations under PHIA or the regulation under PHIA, enactments for which the department itself is responsible. The department also did not comply with its own PHIA policies and procedures. Our office recognizes that the department has implemented improvements to its privacy management program since the discovery of the breach.

The eleven recommendations in this report are intended to assist the department in ensuring that it complies with its statutory duties. The department has accepted all of the recommendations and has either implemented or committed to implement them.

Intentional unauthorized access to personal health information by an employee is a very serious matter. This investigation report is being published in light of the public interest relating to the prosecution and so that other trustees may benefit from the lessons learned from the investigation.

INVESTIGATION

Scope of the Investigation

Our investigation examined the unauthorized access by the department's employee to the sensitive personal health information of a number of individuals, including family members, acquaintances and professional contacts. We also reviewed the measures in place to prevent, detect and respond to unauthorized access by the employee. This included examining the employee's permissions to access electronic health information systems and examining the department's policies and procedures related to PHIA in order to identify opportunities for improvement.

This investigation was initiated under clause 28(a) of Part 4 of PHIA, which provides that in addition to the ombudsman's powers and duties under Part 5 respecting complaints, the ombudsman may conduct investigations and make recommendations to monitor and ensure compliance with PHIA.

In addition, several of the individuals whose personal health information was accessed exercised their right to make privacy complaints to our office. These individual complaints engaged the ombudsman's authority, under clause 39(2)(a) of PHIA, to investigate a complaint that a trustee (the department, through its employee in PDP) has collected, used or disclosed the complainant's personal health information contrary to PHIA. The act also provides a right of complaint under clause 39(2)(b) about a trustee's failure to protect the complainant's personal health information in a secure manner.

Legislative Framework

Personal health information is universally acknowledged to be among the most sensitive personal information that exists. In order to assure Manitobans that their personal health information will be protected, PHIA and its Personal Health Information Regulation ("the regulation"), impose obligations on personal health information trustees. As a public body that collects, uses and discloses personal health information, Manitoba Health, Seniors and Active Living is a trustee to which PHIA applies.

An employee's accessing or viewing of personal health information that is found in an electronic information system is a "use" under PHIA. PHIA prohibits a trustee from using or disclosing personal health information except in the circumstances allowed under PHIA (subsection 20(1)). The purposes for which the use of personal health information is authorized are described under section 21 of PHIA. Every use of personal health information must be limited to the minimum amount of information necessary to accomplish the purpose (subsection 20(2)).

The trustee also has an obligation to limit the use of personal health information by its employees. The trustee must ensure that its employees only have access to personal health information that they need to know in order to carry out the purpose for which it was collected, unless otherwise authorized under PHIA (subsection 20(3)). Additionally, a trustee must determine which personal health information each of its employees is authorized to access (section 5 of the regulations).

PHIA also requires a trustee to implement "reasonable administrative, technical and physical safeguards that ensure the confidentiality, security, accuracy and integrity of the information" (section 18). These safeguards must take into account the sensitivity of the personal health information (section 19). These safeguards must include implementing controls that limit the persons who may use personal health information to those specifically authorized by the trustee to do so and that prevent personal health information from being used unless the identity of a person trying to use it is verified as a user authorized by the trustee (subsection 18(2)). The controls must also ensure that the information cannot be used unless the proposed use is verified as being authorized under the act.

The regulation under PHIA imposes other obligations to protect personal health information and the following are relevant to this investigation:

- A trustee must have, and comply with, written policy and procedures addressing the following (section 2):
    - the security of personal health information during its use, disclosure and storage (among other things)
    - recording of security breaches
    - corrective procedures to address security breaches

- In accordance with guidelines of the minister responsible for the administration of PHIA[1] a trustee must create and maintain (for at least three years) electronic or manual records of user activity for any electronic information system it uses to maintain personal health information (section 4). This reflects the fact that electronic information systems can make sensitive information available to more people, and with greater ease of access, than is the case with paper records. The record of user activity identifies the individuals whose personal health information was accessed, the persons who accessed it, when it was accessed, the electronic system in which it was accessed, and whether it was subsequently disclosed.

- A record of user activity is both a technical and administrative measure for safeguarding personal health information. A trustee must audit records of user activity to detect security breaches, again in accordance with the minister's guidelines (section 4).

- A trustee must also provide its employees orientation and ongoing training about its policy and procedures referred to in section 2 of the regulation, regarding the security of information, recording breaches and corrective procedures (section 6).

- A trustee must ensure that each employee signs a confidentiality pledge that includes an acknowledgement that the employee is bound by the policy and procedures and is aware of the consequences of breaching them (section 7).

- A trustee must audit its security safeguards at least every two years (section 8). If an audit identifies deficiencies, the trustee must correct them as soon as practicable.

Description of Relevant Events

The department hired the employee in question on June 6, 2005 to conduct pharmacy audits and investigations under the Prescription Drugs Cost Assistance Act related to Pharmacare. By virtue of January 24, 2006 delegation letters signed by the assistant deputy minister, the employee was appointed as an inspector pursuant to section 75.2 of the Health Services Insurance Act and pursuant to section 10.1 of the Prescription Drugs Cost Assistance Act.

In this role, the employee had access to personal health information in several electronic information systems, as follows:

> ***DPIN (Drug Program Information Network)*** (in online format (auditable) and in Visual Basic (VB), a legacy format, which was not auditable) – This system contains extensive personal information, much of which is highly sensitive personal health information. It includes patient name, gender, birth date, addresses (past, present, temporary) claims made, deductible information, drug history, dispensing pharmacies, prescriber identifying information, Personal Health Identification Number (PHIN), pharmacist's number and Drug Identification Number (DIN) and drug name (generic or brand name) for each

[1] The minister responsible for the administration of PHIA is the minister of Manitoba Health, Seniors and Active Living

prescription, as well as the quantity, strength and days of supply dispensed for each prescription. It includes program coverage information, such as Pharmacare, personal care home, family services and palliative care coverage. It also includes social insurance number (SIN), and current and past income information, obtained from Canada Revenue Agency (CRA), for the head of family and spouse.

IREG (Health Insurance Registry) – This system contains information such as PHIN, Manitoba health registration number (and past numbers), coverage code and date, residency inside or outside Manitoba, power of attorney information, and treaty or band information. It also contains information about 'maiden' (or prior) names, relationship codes, military codes, family size, power of attorney history, notes, and information about permits (work, student, visitor, refugee etc.).

LTC (Long Term Care) – This database contains information such as PHIN, Manitoba health registration number, patient name, gender, birth date, address, admission date, diagnosis on admission, level of care, facility identity, SIN for resident and spouse, CRA income information for resident and spouse.

MC (Medical Claims) – This system contains PHIN, Manitoba health registration number, patient name, gender, birth date, address, and information about medical payments, number of services, health provider and payment amount. Medical payments are described by two different types of codes – 'tariff' codes and 'ICD9' codes (9^{th} revision of the International Classification of Diseases reference). The tariff code is a 4-digit number, which reveals the type of medical visit and the type of practitioner (via the tariff code look-up function integrated into the database). The ICD9 codes also reveal diagnoses or descriptors of medical conditions (via the ICD9 code look-up function integrated into the database).

HCD (Home Cancer Drug) – This database contains information about provision of cancer treatment and support drugs, free of charge, to patients outside of a hospital setting. It contains PHIN, Manitoba health registration number, patient name, birth date, and generic drug name. This would identify individuals who have been diagnosed with cancer.

MDI (Microfiche and Film Document Interface) – This system contains PHIN, Manitoba health registration number, and identifies the location of scanned documents about individuals, thus permitting these documents to be located and viewed.

While these databases exist independently and are described as separate sources of information, our office notes that the user interface through which the information is made available appears to be highly integrated, such that the databases appear either as clickable links on either the top or side of the screen. There are other indicators of integration within the user interface, including, for example, within the IREG system, where the Registry Profile Page for any particular individual has several clickable tabs, one of which is to the DPIN history for the individual.

During 2012 and 2013, the PDP branch noted performance issues on the employee's part, notably involving his initiating or authorizing activities without approval from superiors or informing them. On March 10, 2014, the College of Pharmacists of Manitoba wrote to the then newly appointed executive director of the PDP branch, expressing concerns about the manner in which the employee dealt with others.

On May 12, 2014, the executive director and department representatives met with the employee to discuss his activities. At some point, the employee was asked to list all organizations outside the department to which the employee had been providing personal health information of individuals. He explained that he received requests from a number of outside organizations, including the RCMP and Winnipeg Police Service and other provincial government departments. He told PDP managers that these requests dealt with matters such as registration in the PDP, suspected improper drug use and alleged 'doctor-shopping' or 'pharmacy-shopping' in order to obtain drugs.

He also told managers that he would investigate allegations brought to him and send the results to the organization that contacted him. He was immediately informed that these actions were not permitted under PHIA or under the department's policies. The employee disagreed and claimed that his managers had previously condoned or permitted this, but could not substantiate this claim. As for his failure to obtain prior management approval, the employee asserted that such approval was not required, as in his view he had authority under PHIA, and perhaps otherwise, to do these things.

The employee's conduct and assertions at this meeting prompted senior PDP staff to obtain an audit of user activity report on May 13, 2014, that set out the systems the employee had accessed for the 12-month period from May 13, 2013 to May 13, 2014. This report indicated that the employee had accessed his own personal health information during that time, as well as the personal health information of four family members from current and prior relationships. This included six cases where an individual had his or her personal health information accessed more than five times in the 12-month period in question. By cross-referencing these accesses against work assignments, PDP was able to determine that these accesses were not for work purposes.

On May 13, 2014, employees of the PDP branch, including this employee, were required to review the department's PHIA policies and to sign an updated pledge of confidentiality. For reasons that are not known, but which seem likely to be related to the timing of the employee's meeting with management the day before, the employee refused to sign a new pledge of confidentiality. Another employee, who was tracking completion of the updated pledges, did not report the refusal to management and as a result, no action was taken at the time to address the failure to complete the pledge.

On June 2, 2014, because of its concerns about the employee's behaviour, the department terminated his access to DPIN, IREG, HCD, LTC, MC and MDI. It did not terminate his access to the legacy version of DPIN (VB DPIN) until June 30, 2014. We understand that the delayed cancellation of access to VB DPIN was an internal oversight resulting from the fact that access to this database was not managed by the same area that managed access to all other databases. As user activity in VB DPIN cannot be audited, it cannot be determined whether the employee

accessed VB DPIN between June 2-30, 2014 (or at any other point in time before that period). It is possible that the employee was not aware that his access to VB DPIN continued after June 2, as he objected to having his system access privileges revoked, and several times asked that he be permitted to continue his work with his DPIN access restored. PDP management declined.

On June 23, 2014, a member of PDP's management requested a further audit of user activity report. On June 25, 2014, a report covering a 60-month period was provided. This showed that the employee accessed hundreds of records of personal health information during that period, a number of which appeared to be questionable in relation to the employee's job responsibilities and work assignments. On June 26, 2014, the manager and a human resources representative met with the employee, along with a union representative. The employee was questioned about his authority to access the personal health information of individuals listed in the audit, including family members, professional contacts and others. He also confirmed that he had sometimes printed personal health information that he had accessed. While the employee generally purported to rely on consent for his authority to access the personal health information of these individuals, he said he could not remember if he had obtained consent to access information from specific individuals the manager identified to him. No evidence was ever provided by the employee that any individuals had consented. Regardless of consent, accessing the personal health information for a personal purpose would not be authorized under PHIA.

PDP management made a further request to the employee on June 26, 2014, to sign the new pledge of confidentiality, and the employee again refused to sign the pledge document that the department presented to him.

On Friday, June 27, 2014, the department took the employee's laptop, desktop computer and BlackBerry from him. PDP management also required the employee to provide his systems password at that time.

The department advised our office that on that same date, human resources and PDP management agreed that the employee should be terminated. This was put in motion, but the employee submitted a resignation letter effective immediately, on Monday June 30, 2014.

On June 30, 2014, PDP's executive director emailed all PDP staff to advise them of the resignation. The email informed staff that they should not allow the employee into the building. The employee's building access cards were de-activated that day. Despite this, the department later determined that at around 7:30 a.m. on the morning of July 2, 2014, the employee gained access to his former office building through an unsecured door. More importantly, he was also able, despite his resignation, to log into his still-active user account using a computer in the building. The department obtained a forensic examination of activities on the employee's user account during this time frame, which showed that he appeared to have deleted files from his account.

In retrospect, the department believes that beginning in approximately 2012, the employee's access to the Medical Claims database would no longer have been necessary to perform his employment duties. As this was not identified at the time, he continued to have access to this database.

As mentioned earlier, the VB DPIN database to which the employee had read-only access, does not have the capacity to log user activity at all. This means that any inappropriate access to personal health information through VB DPIN cannot be determined.[2] It appears likely to our office that there was inappropriate access by the employee to this system, because in an email the employee subsequently sent to family members, he appeared to acknowledge accessing records of some individuals whose names had not appeared in either of the audits of user activity that the department had obtained.

The department advised our office that a "regular, random audit process" was established in 2013. It is clear from the information the department has provided to our office that it discovered these actions largely, if not solely, because the March 10, 2014 email from the College of Pharmacists of Manitoba brought concerns to the department's attention.

Based on our investigation, including information we received from the department and our office's review of the materials, it can be concluded that the employee did the following:

1. He disclosed personal health information to outside organizations without the department's approval. These organizations included the RCMP, Winnipeg Police Service and pharmacies.

2. He sent personal health information by email to outside organizations multiple times without encrypting it. The department, for example, identified to our office that on March 4, 2014 the employee sent 102 patient records (apparently including PHIN, name, address and narcotic prescription information) by email to the managing director, Department of Surgery at the Winnipeg Regional Health Authority. This information was not encrypted. Some 327 patient records containing the same types of information were emailed to the same destination on March 6, 2014. This was in breach of the department's own policies, including regarding security measures to protect personal health information[3]. The employee appears to have been aware that encryption was required as he sent a similar email attaching detailed prescription history of an individual (which was encrypted and password protected) on January 30, 2014, only one month before the two unencrypted files were sent.

3. In 2013, the employee sent a fax to all Manitoba pharmacies containing the personal health information of a particular individual and the individual's family members, because the employee wanted to alert pharmacies of a suspicion that the individual might be committing fraud, so that pharmacies could take extra precautions if requested to

[2] The department advised that it has for some time been in the process of transitioning from VB DPIN to the already-operational DPIN web-based application, which does have the capacity to log access to client records.

[3] Manitoba Health Revised Policies and Procedures under the Personal Health Information Act (PHIA) - 2003, 2010, and Policies and Procedures under the Personal Health Information Act "The PHIA Manual" - 2014 all contain a section titled "VIII: Security of Personal Health Information," which state that personal health information can only be sent by email if it is encrypted or sent over a protected computer network, the sender has verified the receiver's address before sending, the personal health information is de-identified to the extent possible, and confidentiality disclaimer is included in the transmission.

dispense prescriptions to the individual or family members. There were several examples of similar faxes being sent. As the employee's job was to audit and investigate pharmacies not individual patients, this type of action was not within the employee's job responsibilities and he appeared to have taken it upon himself without first consulting or obtaining approval from PDP management.

4. He inappropriately accessed his own personal health information and the personal health information of various current and former family members, acquaintances, other departmental employees, employees of outside organizations, and a small number of senior public officials. The department has confirmed that, to its knowledge, these accesses were not part of the employee's employment duties.

To summarize, it is clear that the employee accessed, used and disclosed personal health information in circumstances where authority does not exist under PHIA. It is also clear that he contravened the department's own policies and procedures under PHIA, for example by disclosing personal health information without following the required reasonable security measures by transmitting unencrypted information to outside organizations. These actions constituted multiple privacy violations by the employee.

As the department's own assessment acknowledges, this breach could result in a variety of harms to individuals, such as identity theft and loss of economic opportunity due to stigmatization based on medical condition or other personal history. As the department also admits, this breach could lead to humiliation or harm to reputation flowing from disclosure of medical diagnoses and other health information. This could cause emotional and other psychological distress and harm. Each of these types of harm is significant. Several individuals who complained to our office reported suffering psychological harm and anxiety as a result of the employee's invasion of their privacy. Some individuals also reported fear for their safety stemming from past experiences in their relationships with the employee.

FACTORS CONTRIBUTING TO THE BREACH

It is important to underscore, first, that ultimate responsibility for the breach lies with the former employee, who repeatedly obtained access to personal health information of individuals when he was not authorized to do so. The department, when it eventually discovered the breach, took meaningful and definitive action to deal with the employee. It was moving to terminate his employment and would have done so had he not resigned as a result of the department initiating these steps.

While the employee's actions were ultimately responsible for the breach, the department's own policies, practices and actions contributed to his ability to access sensitive personal health information of a significant number of individuals over a lengthy period. Had the department implemented more robust policies and practices, the employee's improper actions could have been prevented in the first place, or certainly could have been discovered and dealt with earlier.

Management of Employee Access to Personal Health Information

The first contributing factor is the management of user access for PDP employees. As noted earlier in the report, the department acknowledged that by early 2012, the employee would no longer have needed access to the Medical Claims database in order to perform his employment duties, yet his ability to access this system was not revoked at that time. The department advised us that it had in place a system to assign and manage access to personal health information by its employees, including those in the PDP area. It is evident from our inquiries that the DPIN database is capable of assigning access permissions. This consists of a toggle function in the associated software application. A supervisor has the ability to select access permission for a specific employee. The department advised that this is done when the supervisor considers that an employee has a need to have access to personal health information to perform his or her functions. Changes to an employee's access profile are made by 'access coordinators' in each business area of the department, who log into the online security access system to enter a request to grant or remove access to any particular system for any particular staff. The request is then processed by an IT security administrator in the department. Such changes are usually made within 24 hours, but can be processed immediately if required.

The department's 2010 *Policies and Procedures Under The Personal Health Information Act* ("2010 PHIA policies"), which were in force at the time the breach was discovered, addressed this issue to a certain degree. Policy V ('Use') provided as follows:

> ***Minimum Amount***
> *When using personal health information, the Department will limit the use to the minimum amount of information necessary to accomplish the purpose for which it is used. This requirement applies even where the use is otherwise authorized under PHIA and this policy.*
>
> ***Restrictions on Employees***
> *Employees must be authorized by branch directors to access and use personal health information. This authorization must be based on an employee's previously defined role and function and must be necessary to that role and function.*
>
> *Employees are prohibited from attempting to access or use information to which they are not entitled.*[4]
> *…*
>
> ***Record of Uses***
> *Each branch must maintain records of the purposes for which personal health information is used, who uses it and the authority for the use under PHIA or another act of Manitoba or Canada.*

[4] The department has revised its 2010 PHIA policies in this respect. Policy V now explicitly requires employees to only access and use personal health information that "they need to access or use in order to perform any specific task or function that they are authorized to perform." This policy also now expressly prohibits employees from accessing, or attempting to access, information without authorization, including their own personal health information and that of a family member, friend or co-worker.

The above requirement to maintain a record of uses is distinct from the records of user activity required by section 4 of the PHIA regulation. The 2010 PHIA policy itself made this clear, and Appendix H dealt with records of user activity.

In addition to policy V ('Use'), policy VIII ('Security') of the 2010 PHIA policies addressed the security of personal health information, including as follows:

> *Branch directors must identify which of their employees are authorized to access personal health information. Employees may only have access to the minimum amount of information they require to fulfil their responsibilities (see the Use of Personal health Information Policy).*

Based on our investigation, a key issue that arises is PDP's management of user permissions and specifically, the overall governance of access permissions. PDP did not maintain a matrix to govern the assignment of user access permissions based on job functions. As noted, policy V required branches to ensure that authorization was "based on an employee's previously defined role and function" and that use of personal health information "must be necessary to that role and function." This speaks to a case-by-case approach to access permissions. The preferred approach is to carefully assess at an organizational level, job function by job function, in order to determine which employees truly need access to personal health information, the extent of that access (field by field), and the nature of the access (read-only, read-write). The end result should be an organization-wide role-based access matrix. The matrix should identify data fields, roles and functions, the nature of the access, and the reasons why access is necessary, role by role.

By contrast, the only records of user access permissions maintained by PDP at the time consisted of the information generated by a supervisor's selection of the permission option in the software application. While it would be possible to construct from this a picture of all access permissions, there was no free-standing matrix or registry, detailing which employees had access to which personal health information and for what purposes. The department's own policy V contained the following requirement (which is unchanged between the 2003, 2010 and 2014 policy versions):

> ***Record of Uses***
> *Branch must maintain records of the purposes for which personal health information is used, who uses it and the authority for the use under PHIA or another act of Manitoba or Canada.*

This policy required PDP to maintain records of access permissions, but such records were not maintained.

PDP did not have a clear, comprehensive and branch-wide picture available to management of who had access to what and for what purposes. Such an overview is important from the perspective of ensuring that only those with a true need-to-know have access to personal health information, and that access is limited to the minimum amount needed to do their jobs (and to comply with the department's own policy V).

A matrix or registry of user access would also record who has read-only access and read-write access. This latter feature is important in light of, among other things, the department's duty under PHIA to take steps to ensure that personal health information is accurate and complete (section 16), and the related right of individuals to seek correction of their own personal health information (Part 2).

Our office acknowledges that the department has, since discovery of the breach in 2014, revised its PHIA policies and procedures. The department adopted a revised version that came into effect on November 5, 2014 ("2014 PHIA policies").[5] This version tightens the obligations of individual employees respecting their access to and use of personal health information. However, room for improvement remains, specifically in relation to the creation and maintenance of role-based access matrices and their administration. The policy should be enhanced to ensure that these measures are required and completed.

We note that Appendix C to the 2014 PHIA policies, which is an annual policy compliance checklist, contemplates annual review of access permissions. Reference is made to annual reviews to "ensure that employees have been granted access to systems only if and to the extent required to perform their duties." The checklist cites the 2014 PHIA policies as the related policy (Policy VIII 'Security'), and it provides as follows:

> *Branches must notify the Department's IT Security Officer as soon as practicable when:*
> *- an individual's employment is terminated, or*
> *- an employee's duties change and the change may affect their need to access departmental health information systems to perform their duties.*

This policy requirement, while helpful, seems more focused on ensuring that day-to-day changes in employment status and employee access needs are addressed in a timely manner. It does not fully satisfy the observations made above about creation and maintenance of a role-based access system. Therefore, the department's policy on maintenance and administration of user permissions requires improvement.

Auditing Employee Access

The second factor that contributed to the breach relates to auditing of access to ensure that only authorized access is occurring and to take action when it is not. To meet both legal obligations and public expectations around protection of personal health information, a trustee such as the department should regularly conduct random audits according to a carefully designed audit program to ensure that only authorized access is occurring. Our investigation disclosed that PDP did not do this at the time of the breach.

Rather, as previously mentioned, the breach came to light because the College of Pharmacists of Manitoba expressed concerns to PDP about the employee's actions. It was only then that PDP began a structured assessment of the employee's behaviour and actions. PDP reviewed reports of

[5] A further revision of the department's PHIA policies took place on December 10, 2015. It appeared to contain minor wording changes, for example the phrase "All Branches must…" replaced "Branches must…".

his user activity only after meetings with him enhanced concerns about his behaviour and actions.

Section 4 of the PHIA regulation requires the department to keep a record of user activity showing what personal health information has been accessed, when this occurred, and which employee accessed the information. Section 4 also requires that a trustee such as the department audit records of user activity "to detect security breaches," which applies to this situation.

Section 4 requires trustees to maintain records of user activity and perform audits, in accordance with the minister's guidelines for auditing records of user activity[6]. We note that the department that set these guidelines did not comply with them. Nor did the department's own policies address this adequately. Appendix H to the department's 2010 PHIA policies refers to the duties under section 4 of the PHIA regulation. It also defines the terms "auditable event," "focused audit" and "random audit." It sets out "guidelines", however, these guidelines appeared to simply re-state the requirement of the PHIA regulation: "a Trustee will establish a process for auditing records of user activity based on the following guidelines." The 2010 PHIA policies did not establish department-wide or branch-specific audit programs.

If the department had established an audit program, the employee's improper actions might have been identified earlier and could have been stopped. This deficiency in our view contributed to the breach and, at the very least, to the extent and duration of the improper accesses.

Some of the department's systems had already been set-up to flag "same-name" user accesses for subsequent review, on the premise that these types of accesses may in some cases be reflective of employees accessing information about family members or relatives, presumably for personal, rather than work-related purposes. Such accesses must be reviewed to determine if they are for a legitimate work purpose or if they are indeed inappropriate. Reports of suspect accesses within these systems were automatically generated to a secure electronic folder, to which managers could log into to review these reports.

Supervisors and managers of PDP that we spoke to during our investigation were not aware that this system was in place and therefore, although several reports were generated over time with respect to this employee, the department's systems show that none were accessed, with one exception. A report about the employee's "same-name" access from February 2014 appeared to have been accessed by a supervisor in another area of the department; however, that supervisor has said she did not do so. Regardless of what did or did not occur, this underscores the need to ensure that PDP and all other branches of the department have in place an effective program of auditing (including random and targeted audits) and that this program is diligently and consistently applied.

It is relevant at this point to assess the approach taken in the 2014 PHIA policies, which were in the process of being updated and which came into effect after the breach was discovered. Policy XI Records of User Activity provides as follows:

[6] This refers to the minister responsible for PHIA, which is the Minister of Health, Seniors and Active Living

> ***Creating and Auditing Records of User Activity***
> *Pursuant to s. 4(1) and s. 4(4) of the Personal Health Information Regulation, branches that are responsible for a health information system that maintains personal health information must create and maintain, or have created and maintained, a record of user activity for each electronic information system it uses to maintain personal health information, and in consultation with the [department's] Legislative Unit[7], must establish a procedure for conducting audits of records of user activity to detect security breaches in accordance with the Guidelines for Records of User Activity (RoUA).*

The Guidelines for Records of User Activity mentioned here consist of guidelines issued by the department to guide all trustees under PHIA, including the department itself. The version approved and effective June 4, 2014 – after the breach occurred – contains guidance on designing and implementing audit programs. As the guidelines state:

> *Auditing records of user activity enables Trustees to assess compliance with organizational and legislative requirements by detecting unauthorized access to personal health information maintained in electronic information systems by authorized system users.*

The guidelines provide useful advice on the design of random audit programs, notably by specifying various audit triggers that must be considered in designing a program. These include, but go well beyond, the same-name look-up capability found in DPIN. The guidelines also specify key issues and risks to be assessed in determining the frequency of random audits, with this overall guidance:

> *Random audits must be of a frequency that reasonably would be expected to act as a deterrent to inappropriate access to and use of personal health information.*

With respect to the department's compliance with PHIA, the 2014 PHIA policies were not accompanied by procedures or other types of practical guidance to branches about how to create, implement, monitor and/or update audit processes for monitoring records of user activity. Neither the 2010 nor 2014 policies contained mechanisms to ensure that individual branches had complied with the department's own guidelines and policies.

The department as a whole is a trustee under PHIA. Yet in this area, as in others, the department's policies set out a decentralized approach, leaving it to individual branches to create their own compliance programs and implement them. This invites fragmentation, inconsistency of approach and confusion. This illustrates why, in the view of our office, a much more robust program for privacy management is needed within the department. This theme is addressed in the discussion of privacy management and compliance later in this report.

During our investigation, and subsequent to the development of policy XI (Records of User Activity), the department developed and implemented practical and concrete guidance in the

[7] The Legislative Unit provides leadership, advice and support to the department on the development of new or amended legislation and regulations, co-ordinates the department's response to requests for access to information under FIPPA and provides education and training on and responds to inquiries under PHIA.

form of creating templates for its branches to use to develop auditing processes for both random and focused audits of records of user activities. These templates were first developed in May 2015 and most recently updated in June 2016. Branches are to work with the department's Legislative Unit to develop their own processes, suitable to the systems and information they hold.

The department also developed specific Security Breach Management Checklists for four different types of scenarios: (1) Administrative Security Breaches; (2) Internal Privacy Breaches; (3) External Privacy Breaches; and (4) Technical Security Breaches. Type 2, which deals with internal privacy breaches, includes scenarios where there has been inappropriate access or use of personal health information by an employee of the department. It requires, among other things, that such instances be reported to the department's Legislative Unit, and investigations of such matters must be conducted in consultation with the Legislative Unit.

These reporting requirements will enable the Legislative Unit to track these types of breaches, including breaches detected by auditing of user activity.

Legacy Systems

Legacy systems pose challenges for ensuring that access to personal health information is for authorized purposes because these systems have limited or no auditing capabilities. Policy IX of the 2014 PHIA policies creates an exemption for the department's legacy systems. The department's guidance to all other trustees under PHIA, in the form of the Guidelines for Records of User Activity, contains the same exemption.[8] The following exemption appears in the 2014 PHIA policies:

> ***Exempt Systems***
> *Legacy systems (ex: systems that were in place or being implemented prior to December 12, 2000) are exempt from the requirement*

It should be noted that legacy systems were first recognized in the PHIA regulation in 2001 and included a requirement for electronic systems designed or acquired after December 11, 2000, to have the capability of producing records of user access. In 2005, the relevant section of the regulation was repealed but we were advised that trustees continued to apply the December 2000 date to legacy systems. However, the ministerial Guidelines for Records of User Activity include a statement that trustees should work toward compliance when considering any upgrades to non-compliant legacy systems.

As noted earlier, VB DPIN lacks any capacity to generate and maintain records of user activity and it cannot be audited. With respect to VB DPIN, the department advised us that VB DPIN continues to be used because it contains functionalities not found in DPIN. It also advised that the phase-out of VB DPIN continues. In view of the VB DPIN weaknesses, the department has

[8] Section 4(1) of the PHIA regulation provides that a record of user activity must be maintained "for any electronic information system it uses to maintain personal health information." The same section provides that this is to be done "[i]n accordance with guidelines set by the minister."

limited the number of employees who have access to it. Our office encourages the department to phase-out VB DPIN as quickly as practicable.

Confidentiality Pledge

A pledge of confidentiality is an administrative safeguard to ensure that employees are aware of, and agree to abide by, the trustee's privacy policies and procedures. Section 7 of the PHIA regulation sets out the requirement for employees to sign a pledge of confidentiality:

> *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.*

Policy VII of the 2010 PHIA policies also required the following:

> *Human Resources will ensure that all new employees are aware of The Manitoba Health Policies and Procedures Under the Personal Health Information Act and sign a Pledge of Confidentiality [Appendix B] as a condition of their employment.*
>
> *Human Resources will also ensure that new employees are aware of the consequences of contravening PHIA and/or the Policies. Depending on the severity of the breach, consequences may range from disciplinary action to termination of employment.*

We were advised that the employee in question was, on or about May 13, 2014, required to sign a pledge of confidentiality, but refused. The department acknowledged that another employee tasked with obtaining his signature did not advise PDP management or human resources of the refusal. In view of the fact that the pledge is a condition of employment, this lapse in ensuring the employee signed the pledge is notable. If PDP management had been notified of this in a timely way, it could have prompted management to question why the employee refused. This could have led to further inquiries and perhaps earlier discovery of the breach. The employee again refused to sign the pledge on June 26, 2014. By this point, however, PDP had good reason to believe the employee had breached the substance of the pledge.

It is also notable that we were unable to locate a PHIA pledge of confidentiality completed and signed by this employee at any point during his employment. The employee's direct supervisor and director in the PDP area did not have signed pledges for this employee, as they were new in their roles and had limited information onsite regarding the employee. In addition, the employee's HR file (with the Civil Service Commission) did not contain any such pledges, only the employee's signed oath of office. We note that policy X (PHIA Orientation and Ongoing Training) of the 2014 PHIA policies now requires that pledges signed by employees at commencement of employment and after ongoing training, are to be kept in the employee's HR file, with a copy of each being maintained by the employee's branch.

THE DEPARTMENT'S BREACH RESPONSE

In light of the serious harm that could stem from this privacy breach, our office assessed the adequacy and timeliness of the department's actions in the wake of its discovery in May and June of 2014:

1. It is clear that the department failed to take steps to ensure that the former employee's user permissions for its information systems were immediately cancelled on the same day as his resignation. This should have been the case.

2. The department's building security either had gaps or mistakes were made that allowed the former employee to improperly enter the office building, *i.e.* to trespass. The department did not discover the inappropriate access to the building until October 2014. This permitted the employee to access his computer account and delete files in the two-day window between when he ceased to be employed and the date his system access was in fact terminated.

3. The department became aware of some aspects of the privacy breach by June 2014 and began an internal investigation. It provided verbal notice of the breach to our office on October 17, 2014, and provided our office with details in writing in late November 2014.

4. The size and duration of the breach appeared to cause significant difficulties for the department in determining exactly what happened and which individuals were affected. The department conducted a five-year audit of the employee's user activity, which was also reviewed by our office. While the department was able to identify 12 affected individuals, our office subsequently identified eight other potentially affected individuals. At our request, the department reviewed these eight and determined that two of the eight individuals required notification.

5. The department issued written notification to the first group of affected individuals months after the audit was obtained. Additional individuals were confirmed to have been affected and were subsequently notified by the department.

This last issue is illustrated by the department's October 2014 internal investigation report provided to our office at the end of November 2014, in which it indicated that it "was determined that a significant amount of investigative work regarding the extent of the breach, the gaps in internal security that enabled the breach, and the processes that the Department is working on to tighten policies and procedures would need to be completed in order to appropriately report the issue to the Ombudsman."

While it is evident that the duration and scope of the breaches committed by this employee posed unique challenges for the department's investigation, notification of individuals should have been a much higher priority. It is not necessary for a trustee to fully complete an investigation before notifying affected individuals, as the purpose of notification is to allow individuals to take steps to reduce harms that may arise from their information being compromised. The sooner the individuals know, the sooner they will be in a position to take steps to protect themselves. It is

also not necessary for a trustee to complete its investigation and complete any internal processes to address policies and procedures before it notifies our office of the breach. While it is not mandatory to report privacy breaches to our office under PHIA, it can be beneficial to a trustee and to the public as we are often in a position to identify issues that need to be addressed in the trustee's efforts to contain and respond to the breach, as well as identifying opportunities to strengthen a trustee's practices to better protect personal health information and prevent future similar breaches.

The significance of how long it took the department to identify and notify affected individuals is illustrated by one example alone. It was determined that the employee accessed the personal health information of an individual who had legitimate personal safety concerns regarding the employee, such that notification should have been given promptly to allow the individual to take steps to protect their safety and security. It is critical for trustees to move promptly and diligently to identify those affected and assess potential risks. In many cases, those risks cannot be fully assessed except by the affected individuals and prompt notification to them is essential. While the department's good faith is not in doubt, their efforts should have started much sooner and been given higher priority.

Our office's review of the department's five-year audit of user activity identified numerous other individuals whose personal health information might have been inappropriately accessed by the employee. The department ultimately was not able, however, to conclude with confidence whether the majority of these individuals were in fact affected. It was not able to tell with certainty whether access to their personal health information was legitimate, *i.e.*, necessary for the employee to perform his assigned work duties. After much investigation effort by the department and our office, two additional individuals were ultimately determined to have been affected, and were notified by the department in early August 2015. Since it is not reasonably clear that personal health information of other individuals was improperly accessed by the employee, no further notifications were warranted.

This aspect of the matter again underscores the need for the department to implement better access controls and to improve its after-the-fact audit and monitoring capabilities for personal health information systems. It is vital that the department not be in a position in the future where it cannot reasonably determine whether or not a particular access to personal health information was authorized. This speaks also to the need for robust role-based access systems and not just retrospective audit capacity.

In this regard, we note that the department's internal Privacy Impact Assessment (PIA) Guide and Tool, the current version of which became effective in 2016, specify the development of "user access role tables" in order to fulfill the requirements of subsection 20(3) of PHIA, to determine authorized access for each of its employees and agents. These documents include guidance around the development of such tables, and include an example table for reference. The PIA tools are to be used when there is a new electronic information system being developed, when modifications are made to an existing system, and for electronic information system initiatives for which the department is the trustee, or is a partner in the initiative.

In its breach report, the department identified the following steps as "long-term strategies" it intended to "implement to correct the situation." The department indicated in the breach report that before the incident it "had already initiated a review of departmental PHIA policies and procedures." It did not provide particulars of the scope, timing or intended outcome of this review, but did identify specific changes that either had already been made "or have been made in response to this specific situation."

1. The department had, prior to discovery of the breach, "already begun a review of its auditing processes and has been working with branches to develop comprehensive auditing policies/procedures." As noted earlier in this report, the department has since developed a Record of User Activity (RoUA) Auditing Process Template, effective June 2016. It is not clear what progress has been made by branches in developing their own processes based on this template, or to what extent branches have implemented their processes and conducted audits.

2. PDP would continue to improve policy and processes within PDP, specifically processes to be followed for disclosing personal health information for law enforcement purposes, and investigative processes within PDP.

3. The department modified two of its personal health information policies, one dealing with use of personal information (policy five) and one with security of personal health information (policy eight). The latter involved only a change to "ensure prompt removal of access to [MHSAL] systems when an employee's duties change and the change may affect their need to access departmental health information systems to perform their duties."

In representations to our office, including the department's breach report, the department identified the following actions that PDP was taking at that time in addition to investigating the breach:

1. It had been working with legal counsel to send notification letters to affected individuals. These were sent in November 2014.

2. It was conducting monthly audits of user activities for all employees that have access to personal health information.

3. It had reviewed the access permissions for each employee to ensure that only employees who needed access to personal health information to do their work had access.

4. It was reviewing the process that it uses to grant employees access to personal health information.

5. It was providing PHIA training to employees who had not received PHIA training in the past two years. The department has since developed an online PHIA training program for its own employees, which is available through Organization and Staff Development, the entity that delivers learning programs to Manitoba government departments. This training

program came into effect at the end of 2015. An online PHIA training program for other trustee organizations and individuals was developed and made available in 2014.

6. It was reviewing the "algorithms of…user access logs to ensure there is enough sensitivity and specificity to identify potentially inappropriate access." This consideration is now included in the department's RoUA Auditing Process Template, which became effective June 2016.

7. It was finalizing a new policy respecting the process of audit and investigations in PDP to ensure that greater clarity existed with respect to job functions associated with the PDP audit/investigations process, which would allow unauthorized access to be more readily distinguished from authorized access.

The department's breach report also said that the department was revising its PHIA policies and procedures to include new policies respecting reporting and management of breaches, auditing programs and annual reporting by branches on their PHIA compliance.

At the time the department discovered the breach, its PHIA policies (version effective 2010) contained minimal guidance on how to respond to privacy breaches. Policy VIII (security) stated that any employee who became aware of a breach had to immediately take steps to cease or lessen the breach and report it to the branch director. The policy also stated:

> *The branch director will consult with the Legislative Unit to determine the steps necessary to correct the breach, if applicable, and to prevent similar breaches from occurring in the future. Branches must also determine whether to provide notice of the breach to any person affected by it and to the Ombudsman.*
>
> *Where technical security safeguards have been compromised, branch directors must also notify the Department's IT Security Officer.*

This policy did not provide guidance on the criteria for determining if affected individuals should be notified, when or how. The same comment applies to determining whether to report a privacy breach to our office. Since 2007, guidance on both of these subjects has been available from our office in the form of two practice notes published on our website – *Reporting a privacy breach to Manitoba Ombudsman* and *Key steps in responding to privacy breaches under FIPPA and PHIA*.

Our practice note on reporting a breach to our office advises trustees and public bodies that breaches should be reported as soon as possible. While it is not mandatory to report privacy breaches to our office under PHIA, it can be beneficial to a trustee and to the public as we are often in a position to identify issues that need to be addressed in the trustee's efforts to contain and respond to the breach, as well as identifying opportunities to strengthen a trustee's practices to better protect personal health information and prevent future similar breaches. It is therefore not necessary for a trustee to complete its investigation and complete any internal processes to address policies and procedures before it notifies our office of the breach.

Our practice note on key steps in responding to privacy breaches (effective 2007, updated and expanded in 2017) contains detailed descriptions of factors to consider at each stage of responding to the privacy breach. In addition to addressing individual notification, our practice note emphasizes the importance of responding immediately to the breach, including by assessing the need for notification. In this case, the department acted to terminate the employee's employment and terminated his access to personal health information, with the exception of his access to VB DPIN that was inadvertently not removed at the same time as his other access privileges were revoked. However, the remainder of its response, particularly its notification of affected individuals, did not proceed as quickly as it should have.

IMPROVING PRIVACY MANAGEMENT AND COMPLIANCE

We note that since this privacy breach, the department has made significant improvements to its privacy management processes. In particular, it has developed extensive guidance for its staff about responding to privacy and security breaches, including checklists for managing administrative security breaches, internal privacy breaches, external privacy breaches and technical security breaches. It has also developed an internal security breach reporting form and an external security breach reporting form, as well as a specific form for reporting privacy breaches to our office. All of these references are available on the department's intranet and help guide staff and branches through these processes. The department has also developed a Record of User Activity Auditing Process Template, enabling its branches to develop their own processes, and presumably, to commence their own auditing programs.

The department's current PHIA policies, procedures and reference material make clear that its Legislative Unit continues to play a central role in terms of providing PHIA expertise and guidance to branches and employees. However, the Legislative Unit does not appear to have management or governance authority. Each branch is expected to ensure compliance, but there is no expressly mandated central governance authority.

A key aspect of this case is the impact of the department's branch-by-branch approach to privacy management. While there may be some advantages in terms of flexibility, as suggested earlier this can lead to fragmentation, inconsistency, confusion and failure to ensure individual branches' compliance with PHIA or the department's own policies. The findings in this report illustrate the need for a more robust privacy management and governance structure in the department. In our view, a centralized approach to privacy management could help to address the concerns identified in this report.

The department should consider appointing a chief privacy officer at a senior executive level to be responsible, in consultation with branch heads, for the co-ordination and management of all aspects of the department's privacy responsibilities.[9] This need not be a new position, but someone with relevant experience, management experience and executive-level profile (and support) should be tasked with this role. Related policy and management responsibility changes would also be needed in order to make this new role work properly. In conjunction with these

[9] This would extend to compliance with privacy duties under the Freedom of Information and Protection of Privacy Act.

steps, the department should undertake a thorough review of its existing privacy management and governance structure.

The department should inventory and assess its personal health information holdings in order to ensure that it is complying with PHIA. This would identify what information is already held, what data elements are being collected, used and disclosed, the authority for these activities, security measures and retention periods. This inventory will provide a granular snapshot of compliance and enable the department to move forward with the creation and implementation of user access controls (role-based access), an audit program and other compliance measures.

The department also should assess its PHIA policies and procedures in light of this report and its recommendations. This review should await the potential new governance and management structure, and appointment of a chief privacy officer.

RECOMMENDATIONS

In light of the investigation findings, the ombudsman made several recommendations to the department. The following incorporates the department's responses to our recommendations:

Chief privacy officer

1. The department should consider appointing a chief privacy officer at a senior executive level. This official should be responsible, in consultation with branch heads, for the co-ordination and management of all aspects of the department's privacy responsibilities.

   Department's response: *This recommendation is very timely since the health system provincially is being reorganized and issues related to information management and governance are being examined at a provincial level.*

New compliance and governance approach

2. The department should undertake a thorough review of its existing privacy management and governance structure. This review should be pursued with the goal of creating a more centralized and co-ordinated approach to privacy compliance and management, noting the concerns identified in this report.

   Department's response: *This recommendation is very timely since the health system provincially is being reorganized and issues related to information management and governance are being examined at a provincial level.*

Inventory of personal health information holdings

3. The department should complete an inventory of its personal health information holdings to ensure that it is complying with PHIA. This should identify what information is already held, what data elements are being collected, used and disclosed, the authority for these activities, security measures and retention periods.

Department's response: *This recommendation is accepted. However, given the health system transformation that is underway, no timeline for completion can be provided at this time as the Department's health information holdings may change as a result of this process.*

Review of policies and procedures

4. The department should review its PHIA policies and procedures in light of this report and the other recommendations made here. This should await the new governance and management structure and appointment of a chief privacy officer.

   Department's response: *This recommendation is accepted.*

Records of user activity

5. The department should ensure that its records of user activity are maintained in a form that complies with its current guidance on auditing of records of user activity. In addition, consideration should be given to ensuring that new or upgraded systems can track and capture whether a user has printed or downloaded personal health information as well as information about the date, time, duration and frequency of access by each user, if possible.

   Department's response: *The department will ensure that its records of user activity are maintained in a form that complies with the current guidance on auditing records of user activity. The department will consider the portion of the recommendation relating to new or upgraded systems in the PHIA legislated review already underway.*

Development of audit processes for records of user activity (RoUA)

6. The department should create comprehensive audit processes for auditing records of user activity in relation to personal health information in departmental information systems, if it has not already done so since the development of its RoUA Auditing Process Template. The department should provide our office with copies of all auditing process documents that have been developed. For any auditing processes that are still being developed, the department should indicate when they will be completed.

   Department's response: *This recommendation is accepted and the work on this is well underway.*

Audit program

7. The department should implement the auditing processes that are developed above, including the performance of random and targeted audits of user activity. The department should provide our office with the results of audits completed to date, and going forward, should consider creating an annual report for the previous year's audit program. Such a report should be made publicly available on the department's website.

Department's response: *The portion of this recommendation dealing with the implementation of audits and providing the results of completed audits to your office is accepted and the work on this is nearing completion. The portion of this recommendation suggesting the creation and publishing of an annual report will be considered as part of the above-noted information management and governance activities.*

8. On an ongoing basis, the department should ensure that each record of user activity is audited before the record is destroyed. These audits should be included in the suggested annual report mentioned in recommendation 7.

   Department's response: *The portion of this recommendation dealing with ensuring that each record of user activity is audited before the record is destroyed is accepted. The portion of the recommendation suggesting that these audits be included in the suggested annual report mentioned in recommendation 7 will be considered as part of the health system transformation work currently underway as indicated in the responses to recommendations 1 and 2.*

Privacy management review

9. The department should perform a comprehensive review of its approach to managing its privacy obligations towards Manitobans. The review should audit its personal health information holdings, assess the department's privacy policies and procedures, assess its management structure for privacy compliance and report publicly on that review. The department should implement any recommendations made in that review report.

   Department's response: *As indicated in the Deputy Minister's letter to the Ombudsman, with respect to the recommendations regarding the structure and management of privacy practices and the reporting of same, the health system provincially is in a state of transformation. Issues relating to information management and governance are being examined at a provincial level, and these recommendations will be taken into account in this work.*

Employee training and compliance commitments

10. The department should conduct ongoing training for all employees who have access to personal health information, including in the Provincial Drug Program branch. This training should cover PHIA and the department's own PHIA policies and procedures. Each new employee should receive this training on being hired and existing employees should receive refresher training at least every three years.

    Department's response: *This recommendation is accepted and is reflected in the department's policy respecting staff orientation and training respecting PHIA.*

11. The department should ensure that every employee signs a pledge of confidentiality upon hiring acknowledging awareness of their responsibilities under PHIA, and the department's policies and procedures under PHIA, and agreeing to comply. Pledges should be re-signed

when there are changes to an employee's access to personal health information or job duties, or in circumstances when an employee has not complied with the trustee's policies and/or PHIA.

Department's response: *This recommendation is accepted.*

Manitoba Ombudsman
December 7, 2017