Manitoba Ombudsman

REPORT UNDER

THE PERSONAL HEALTH INFORMATION ACT

CASES 2013-0111 AND 2013-0113 (web version)

WINNIPEG REGIONAL HEALTH AUTHORITY

PRIVACY COMPLAINTS: USE AND DISCLOSURE OF PERSONAL HEALTH INFORMATION

PROVISIONS CONSIDERED: 18(1), 19, 21(a), 22(1)

REPORT ISSUED ON AUGUST 28, 2013

SUMMARY: **Manitoba Ombudsman received a complaint that an employee of the Winnipeg Health Sciences Centre (HSC), a trustee under *The Personal Health Information Act* (PHIA or the act), had improperly accessed and disclosed the complainant's personal health information. Our office investigated the extent of the privacy breach and the actions taken by the trustee in response. The ombudsman found that the employee's use and disclosure of the complainant's personal health information was carried on outside the employee's work related duties and was therefore not authorized by *The Personal Health Information Act*. The investigation of the privacy breach and response by HSC was found to be appropriate in the circumstances. However, we also found that safeguards required by the regulations for electronic health information systems - specifically the capacity to create and maintain of a complete record of user activity – were not in place, thus hampering audit capabilities and the ability of the trustee to conduct a complete investigation.**

BACKGROUND

The complainant was informed by a family member that personal health information relating to the complainant had become known to a third individual. Given the nature of the information, the complainant concluded that her personal health information had been accessed and disclosed by someone working at Winnipeg Health Sciences Centre (HSC) and the complainant suspected that a particular individual was responsible. The complainant reported her suspicion to the HSC privacy officer on February 25, 2013. The HSC privacy officer undertook an investigation and immediately moved to audit access to the complaint's health information records on the main systems to which the suspect employee had access. These included the Admission Discharge Transfer system or ADT system and the Provincial Client Registry of Manitoba Health (PCR).

As a result of the system audits and subsequent questioning of the employee, HSC concluded that the employee had accessed the personal health information of several individuals[1] including the complainant for an improper use thereby violating the requirements of PHIA for personal health information trustees. The HSC investigation also concluded that there was reason to believe that the employee disclosed and shared the complainant's personal health information to a person outside the hospital.

The behaviour engaged in by the HSC employee in this case is commonly referred to as "snooping." Snooping ranges from viewing (and possibly disclosing) the health records of celebrities or other well known individuals who are not personally known to the snooper, to accessing the health records of family members, acquaintances or the family members of acquaintances. In some cases, the personal health information viewed by the snooper is then disclosed in a way that can cause embarrassment and other harm to the subject of the record. Details of the circumstances around the use and disclosure which took place in these complaints cannot be described to protect the privacy of the complainant; however, the violation of privacy which took place in this case is of the most egregious kind.

HSC responded immediately when contacted by the complainant. They quickly investigated and took immediate steps to insure that the complainant's personal health information could no longer be viewed by the suspect employee. A written apology was made to the complainant on March 12, 2013.

[1] The complainant and the other individuals whose personal health information was also viewed inappropriately are known to each other and are aware that each other's privacy had been breached.

THE COMPLAINTS

The Personal Health Information Act provides an individual with the right to make a complaint to ombudsman about a breach of privacy under subsection 39(2), which reads:

> **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.

Two complaints concerning the improper use and disclosure of personal health information by an employee of HSC outside the employee's work-related duties and contrary to PHIA were delivered to our office by the complainant in this case on March 25, 2013. In such cases where the privacy breach has been found to have already taken place, our investigation examines the actions of the employee as well as the actions and responsibilities of the personal health information trustee in the context of the law and the regulations governing personal health information in Manitoba. This will also involve assessing the trustee's actions in response to the initial complaint of a privacy breach.

INVESTIGATION

In privacy breach investigations the role of the ombudsman's office as defined under subsection 39(2) is two-fold. Under clause 39(2)(a), we examined the extent of the breach by determining when and why the personal health information of the complainant was accessed and disclosed by the employee. This also involved examining the type and sensitivity of the information housed in the HSC records systems to which the employee had access.

Under clause 39(2)(b), we examined whether the trustee took appropriate security measures to safeguard the personal health information of the complainant in a secure manner as required by PHIA. Security measures include written security policies and procedures established by the trustee, access restrictions and any additional safeguards specific to electronic health information systems.

Our office also reviewed the steps taken by HSC and the Winnipeg Regional Health Authority (WRHA) when alerted by the complainant that a breach may have taken place. The WRHA is the trustee of the personal health information collected and maintained within the health care facilities it owns and operates, including HSC. The WRHA developed (and oversees compliance

with) the privacy policies in effect for all WRHA facilities. For the purposes of our investigation, our office collected information from the complainant as well as written and oral representations from the WRHA and HSC.

HSC Employee's Use and Disclosure of Personal Health Information

PHIA defines personal health information as follows:

> "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;

PHIA stipulates that a trustee (and, by extension, the trustee's employees) may use personal health information only for the purpose for which it was collected or received. Section 21 of the act contemplates situations where personal health information may be used for another purpose but these are strictly defined and limited by the act and all relate to the provision of health care and associated services. When use of personal health information is not authorized under section 21 of PHIA, the use constitutes a violation of privacy under the act.

PHIA contains similar restrictions concerning the disclosure of personal health information:

> **Individual's consent to disclosure**
>
> 22(1) Except as permitted by subsection (2), a trustee may disclose personal health information only if
>
> (a) the disclosure is to the individual the personal health information is about or his or her representative; or
>
> (b) the individual the information is about has consented to the disclosure.

Subsection 22(2) of PHIA sets out situations where personal health information may be disclosed without consent but as with use, the circumstances for disclosure under PHIA are strictly defined

and limited by the act. When disclosure of personal health information is not authorized under subsection 22(2) of PHIA, the disclosure constitutes a violation of privacy under the act.

The requirements of PHIA apply whether the information is in a paper or electronic record. Accessing and viewing personal health information in an online record system constitutes a use under PHIA. Making the contents of that record known to someone not employed or otherwise contracted by the trustee constitutes disclosure under PHIA.

Additionally, PHIA places an obligation on health care trustees to limit the use of personal health information by its employees as follows [emphasis ours]:

> **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**.

At our request a copy of the HSC employee's job description was provided to our office. The HSC employee at the centre of this case worked in hospital admitting and patient registration. The job description indicates that this individual would be familiar with health records as well as various electronic systems. These include systems used for scheduling outpatient appointments (the MSI system), the system which tracks hospital admissions, discharges and transfers (known as either the ADT or the ATD system)[2] and the Manitoba Health Database of Insured Manitobans (also known as the Provincial Client Registry or PCR system). According to the supplied job description, this employee would collect demographic data from patients as well as financial information relating to payments for services and insurance coverage. The HSC employee would also incorporate defined elements of patient data for ambulatory care patients into the HSC patient index, register new patients and update the patient's encounter history and demographics (name, address, telephone number, and email address)[3] on existing indexed patients. The employee in this case would not normally have a reason to access patient charts or the results of diagnostic testing (which are held in other systems). However, there are employment related instances where this would be necessary.

The employee's responsibilities could also involve providing registration information to Vital Statistics and other public agencies.

One of the main functions of the position as stated in the employee's job description supplied to our office is "maintaining patient confidentiality at all times in accordance with Winnipeg

[2] For the purposes of consistency, this system will be referred to as the ADT system throughout this report.
[3] As defined by PHIA.

Regional Health Authority (WRHA), Personal Health Information Act (PHIA), policy and contractual obligations." The job description also states the employee "adheres to all corporate and departmental policies and procedures." These statements demonstrate to our office an appreciation of the sensitivity of the information, which relates to surgical and other inpatient/outpatient procedures and ongoing treatment that would be handled by the HSC employee in this investigation.

The primary system with which the HSC employee worked was the ADT system. Our office found that the ADT system may contain[4] the following information:

- Primary demographics (last name, given names, HSC registration number, Manitoba Health registration number or PHIN[5], date of birth, sex).
- Biographics (address, phone number, social insurance number, known aliases, medic alert, name of next of kin, home care history).
- Encounter history (locations - which are usually hospitals - and dates). Each encounter history may have further associated information (including the admitting diagnosis and the encountering physician's name).
- Inpatient demographic and biographic information (including date and place of birth and religion, name of attending and family physician, reason for admission, infectious status, insurance status, employer group, immigration and or visa status, cancer care number).

From this description, our office determined that the ADT record has the potential to contain a great deal of personal and personal health information. That which pertains to the reason for admission, diagnosis, and chronic conditions (as in medic alerts) could possibly be quite sensitive.

In her complaint to HSC, the complainant described the personal health information she believed to have been disclosed. Given the type of information and the position of the employee which the complainant suspected was responsible, the HSC privacy officer concluded that the information disclosed would most likely have come from the ADT record and was unlikely to have come from any other record to which the employee had access.

HSC requested an audit of access to the complainant's ADT record. Review of the ADT audit log did not reveal any inappropriate access (no access of the complainant's ADT record by the employee in question was shown for the time period during which it was believed access took place). However, the HSC ADT system is a "legacy" system. HSC explained to our office that tracking of access is limited to tracking actual changes made to records in the system. "View Only" use of the system is not tracked. HSC concluded that, although there was no evidence of

[4] Data fields into which this information may be entered exist within the ADT system but may not always be filled in.

[5] A number assigned to individuals in Manitoba by the minister of health to uniquely identify individuals for health care purposes.

any changes made to the ADT record, this did not mean that inappropriate access and viewing could not and did not occur.

Another system with which the HSC employee worked frequently was the PCR (Provincial Client Registry) system. Individual records in this system are used to uniquely identify all individuals receiving health care services in Manitoba. The PCR is designed to contain the following information:

- Client PHIN.
- Demographic (name, address, phone number) and other identifying information including birth date, gender.
- Last activity date and facilities in which the client was seen[6]

HSC requested an audit of "Access by User ID" of the PCR system for 2012. The audit revealed that the suspect employee had accessed the PCR record of the complainant and several of the complainant's family members[7] during 2012. As part of the audit and investigation process, HSC also determined that neither the complainant nor the family members had visited HSC on the dates when use of their PCR system records by the employee took place. Access of the complainant's PCR record was not required by the HSC employee on those dates and, therefore, outside the employee's work related activities. HSC then questioned the employee who admitted to accessing the complainant's health information record for a purpose not related to the employee's work related duties.

Although the HSC audit of the ADT system was inconclusive, the HSC investigation also found (based on a balance of probabilities) that the employee disclosed personal health information that was available to be viewed on the ADT system and nowhere else. Currently, it is not an offence under PHIA for an employee of a trustee to wilfully use, gain access to or attempt to gain access to another person's personal health information without the authorization of the trustee.[8] However, subsection 63(2) of PHIA stipulates that an employee, who wilfully discloses personal health information in circumstances where the trustee would not be permitted to disclose information under the act, is guilty of an offence. Still, a higher burden of proof than the balance of probabilities must be satisfied for an offence to be prosecuted under PHIA. Proofs such as physical evidence (copies of pages printed from the complainant's personal health information record) or the sworn testimony of witnesses would generally need to be obtained before an offence prosecution can be contemplated. These proofs could not be obtained in this case, and this a prosecution was not pursued.

[6] Manitoba hospitals have access to the Provincial Health Insurance Registry viewer. The WRHA explained to our office that the viewer does not allow the user to see the field with information on other facilities in which the client was seen.

[7] The unauthorized access of the personal health information of the complainant's family members is the subject of separate investigations and reports by our office.

[8] An amendment to PHIA which would make willfully viewing a personal health information record without authorization an offence under the act was proposed as Bill 4 in the 2nd Session, 40th Legislature.

HSC advised our office that disciplinary action was taken against the employee in this case and the employee was held accountable for her actions in this matter. In human resource matters the HSC is acting as public body under *The Freedom of Information and Protection of Privacy Act* (FIPPA). As such, the HSC is required to limit the disclosure of the personal information of its employees to the minimum necessary to accomplish the purpose for which it is disclosed. In some instances a trustee or public body may be able to share employee disciplinary information with an affected individual but in many cases this would not be consistent with FIPPA. Disciplinary measures are imposed based on a combination of factors relating to employee work history and personal background and not just the matter which may have precipitated the disciplinary procedure. Disclosing these considerations may be necessary to understand the discipline imposed but it could also reveal information beyond the limits necessary for the matter at hand.

Based on the information provided to our office by the complainant and the WRHA, our office was in agreement with the HSC finding which determined that the employee accessed (used) the information deliberately for a purpose not related to her work duties and it is likely the employee disclosed information without authorization. Both the use and disclosure were contrary to the trustee's obligations under subsection 20(1) PHIA. Our office also concluded that the response of HSC to these breaches of the complainant's privacy was appropriate in the circumstances. Our investigation then turned to the trustee's obligations under subsection 18(1) of PHIA.

Security Safeguards Required Under PHIA

To uphold public confidence and support high quality patient care sections 18 and 19 of PHIA stipulate that health information trustees shall take measures to protect the confidentiality, security, accuracy and integrity of personal health information, as follows:

> **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.
> **Specific safeguards**
> 18(2) Without limiting subsection (1), a trustee shall
> (a) implement controls that limit the persons who may use personal health information maintained by the trustee to those specifically authorized by the trustee to do so;

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

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

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

(c) if the trustee uses electronic means to request disclosure of personal health information or to respond to requests for disclosure, implement procedures to prevent the interception of the information by unauthorized persons; and

(d) when responding to requests for disclosure of personal health information, ensure that the request contains sufficient detail to uniquely identify the individual the information is about.

Additional safeguards for information in electronic form

18(3) A trustee who maintains personal health information in electronic form shall implement any additional safeguards for such information required by the regulations.

Safeguards for sensitive information

19 In determining the reasonableness of security safeguards required under section 18, a trustee shall take into account the degree of sensitivity of the personal health information to be protected.

As subsection 18(1) states, the safeguards to be implemented fall into three categories – administrative, physical and technical – to take into consideration all potential risks present in the environment within which the information exists.

As set out in section 2 of *The Personal Health Information Regulation* under PHIA (the regulation) administrative safeguards first and foremost include the establishment of written policies and procedures for the protection of personal health information throughout its entire lifecycle. Policies (and the procedures by which policies are put into effect in the day to day operations of the organization) set out the specific means whereby the health information trustee will comply with the requirements of the act and the regulation. This should also include policies and procedures for detecting and responding to breaches of information security and patient privacy.

Physical safeguards take the form of measures such as using locked cabinets to store files or restricting physical access to the area within which patient information can be viewed. Section 3 of the regulation sets out basic physical safeguards such as ensuring that personal health information is maintained in designated areas and access to such areas is limited to authorized persons. Section 5 of the regulation and subclauses 18(2)(b)(i)(ii) of the act speak to the need to

set out procedures that limit access to personal health information to those authorized to do so, that the identity of users is verified and the use is for a purpose authorized under PHIA.

Policies and procedures are ineffective if employees are not aware of them. Training and awareness activities must be implemented, as required by Section 6 of the regulation, to ensure that policies and procedures are understood and followed. Section 7 of the regulation instructs trustees to obtain a signed "Pledge of Confidentiality" from each employee (or agent) by which the signatory acknowledges that they are bound by the trustee's procedures and policies. Section 8 of the regulation also stipulates that health information trustees will conduct a review and assessment of security safeguards, at least every two years and that steps are taken to correct any deficiencies that are identified as soon as practicable.

Analysis of Winnipeg Regional Health Authority Security Safeguards

In accordance with section 2 of the regulation, the WRHA has established policies and procedures for the institutions which it owns and operates. In considering whether the WRHA protected the complainant's personal health information in a secure manner as required by PHIA, our office reviewed the safeguard measures taken by WRHA. In so doing we took into consideration the requirements of the legislation and the associated regulations.

The WRHA has a comprehensive suite of PHIA policies which have been emulated by other provincial regional health authorities. Our office examined similar policies as part of our investigations into the privacy breach which took place at CancerCare Manitoba in 2011. As a result of our investigation report, the WRHA began a review of their PHIA policies and procedures. This review is ongoing.

Security and Storage of Personal Health Information Policy

We observed that the purpose of this policy is "to ensure that security and integrity measures are in place and followed in order to protect the confidentiality and integrity of personal health information within the Winnipeg Regional Health Authority ("WRHA")." We observed that this policy is primarily focused on the protection of personal health information from external factors such as access by unauthorized personnel and damage from physical threats as required by section 3 and section 5 of the regulation. Among other things, the policy states that:

> Personal health information is to be collected, used, disclosed or accessed only by individuals who are authorized for that purpose. **Individuals thus authorized must have a clear understanding of the authority, parameters, purposes and responsibilities of their access, and of the consequences of failing to fulfill their responsibilities** [emphasis ours].

The employee in this case was authorized to use both the ADT system and the PCR viewer. The policy makes clear that the authority to access personal health information is a work related privilege and with that comes an attendant responsibility to use that access appropriately. We observed, however, that the employee's inappropriate use of these systems indicated that, "a clear understanding of the authority, parameters, purposes and responsibilities of their access, and of the consequences of failing to fulfill their responsibilities" was absent.

Under this policy security safeguards are described to include both physical and human resource safeguards (which would include such measures as security clearances, sanctions, training and contracts to mandate measures taken by agents and information managers). The WRHA has explained that the ADT system is one that is in constant use by more than one person in several administrative areas simultaneously. Thus, we noted that physical security safeguards beyond passwords would be difficult to implement in this environment. However, as has been illustrated by the complaint investigated here, some information contained in the ADT system can be highly sensitive. In the case of this type of widely used system, the HR safeguards such as sanctions and training assume greater importance.

We noted that the procedure associated with this policy states that, "individuals who sign on to a computer must not leave the computer on in accessible areas when they leave their workstation. User password protocols must be in place and utilized. Where possible, automatic shut offs after a prescribed period of disuse should be programmed for all workstations." This procedure makes audits of "User Access by User ID" possible. Without the requirement of a unique password for each employee in order to access to the PCR, it would not have been possible to identify the individual employee responsible for unauthorized access to the complainant's PCR record.

Access to Personal Health Information Policy

We observed that this policy states the trustee shall take steps to inform individuals of their right to request access to their own personal health information (and how they can exercise that right) in compliance with PHIA subsection 5(1):

> **Right to examine and copy information**
> 5(1) Subject to this Act, an individual has a right, on request, to examine and receive a copy of his or her personal health information maintained by a trustee.

As more and more personal health information moves to electronic systems this will include not only the right of access to one's own health record but also to examine the record maintained by the electronic system of who has accessed one's own personal health information, as set out in subsection 7(3):

> **Information in electronic form**
> 7(3) When a request is made for personal health information that a trustee maintains in electronic form, the trustee shall produce a record of the information for the individual in a form usable by the individual, if it can be produced using the trustee's normal computer hardware and software and technical expertise.

The WRHA has explained to us that it is most certainly possible for an individual to request an audit of access to their own personal health information on electronic systems (subject to the limits of the system) and that such records are being provided on request. We note, however, that the complainant in this case was not advised by the HSC privacy officer that she could examine an audit of access to her personal health information records. We also observed that information on how to request or see a copy of one's own personal health information on the WRHA web pages and the WRHA "Request to Access Personal Health Information" form do not mention the right of individuals to make a request for a copy of an access audit.[9] Stepped-up public awareness activities would make it easier for individuals to understand their rights under PHIA. If the access request form and information pages were enhanced to make this clearer, individuals would be better able to take advantage of this resource.

Use and Disclosure of Personal Health Information Policies

We observed the purpose of these policies is "to ensure that the individual's right to Privacy of their Personal Health Information including Demographic Information is protected" during use and disclosure as set out under PHIA as required by section 5 of the regulation and subclauses 18(2)(b)(i)(ii) of the act. In the case of use, this goal is accomplished through a number of policy statements including the following:

> 3.2 A Trustee shall limit the Use of Personal Health Information to those Persons Associated with the Trustee who need to know the information **to carry out the purpose for which the information was collected or received**.

We noted that this policy does not mention the possibility of disciplinary action against employees who violate the policy (although the "Confidentiality of Personal Health Information Policy" does – see discussion following). The "Security and Storage of Personal Health Information Policy" discussed previously states that individuals authorized to collect, use (access) or disclose personal health information "must have a clear understanding of the authority, parameters, purposes and responsibilities of their access, **and of the consequences of failing to fulfill their responsibilities** [emphasis ours]." One of the ways to ensure this is to make clear in the use and disclosure policies that the WRHA will deal with any snooping and/or inappropriate disclosure activity by employees swiftly and with disciplinary sanctions

[9] eChart Manitoba online awareness materials do explain that everyone has a right to know who has viewed their information and a form is also available online to request a record of user access.

appropriate to the severity of the employee's inappropriate behaviour up to and including dismissal with cause. This message cannot be repeated too often.

Reporting of Security Breaches Related to Personal Health Information (and The Corrective Process to be Followed) Policy and Procedure

According to this policy a security breach incident may range from "unauthorized individuals being able to view a computer screen or paper file, to theft or loss of WRHA computer equipment including electronic storage media, to unauthorized destruction of information through a water-main leak." The policy states:

- all breaches of confidentiality should be reported, recorded and analysed;
- corrective procedures to prevent similar breaches should be put in place;
- corrective procedures must be followed.

The procedures for the implementation of this policy set out the process for initiating and investigating a breach. We observed that the procedures also set out,

> If it is determined that a breach of confidentiality of personal health information has occurred, appropriate remedial action shall be taken. Such action may be disciplinary action up to and including termination of employment/contract/ association/ appointment with the WRHA or the Facility where the breach occurred. The supervisor shall consult with the designated representative in Human Resources to establish the appropriate level of disciplinary action to be applied. Further education may be provided to the individual if appropriate.

As noted previously, this procedure was followed and appropriate remedial action was taken in this case.

The procedure further states that the manager/supervisor should "facilitate opportunity to engage staff in a debriefing session and identify corrective procedures." Unfortunately, shortly after HSC completed its investigation into this privacy breach the legacy ADT system crashed and staff were forced to revert to a manual registration system until repairs could be completed. As a result of this system failure (the WRHA explained to our office) HSC administrative staff workloads were dramatically increased in the employee's work area. The demands of maintaining patient care did not allow an opportunity to conduct follow-up awareness activities in a timely manner. It is our view that such measures have significant impact and benefit and should be undertaken whenever possible.

Additionally, the procedure states that the WRHA privacy officer or designate (in this case the HSC privacy officer) receives the occurrence report and makes recommendations for measures to prevent future similar breaches. We note that, following the inappropriate access of the

complainant's personal health information on the ADT system, the HSC privacy officer made a request to enhance the audit capability of the HSC ADT system, specifically to ensure "view only" access was logged. The system failure caused the WRHA to move quickly towards the implementation of an updated ADT system such as those which are already in place in other WRHA hospitals and which would greatly improve audit capabilities.

Confidentiality of Personal Health Information Policy

This policy is listed first among the WRHA's PHIA policies and this may be seen as an indication of how the WRHA views the importance of this policy in safeguarding personal health information. We noted that the following policy statements are particularly relevant in the context of this investigation [any emphasis is ours]:

> 3.1 **All employees and Persons Associated with the Trustee are responsible for protecting all Personal Health Information** (oral or recorded in any form) that is obtained, handled, learned, heard or viewed in the course of his/her work or association with the Trustee.
> 3.2 Personal Health Information shall be protected during its collection, Use, storage and destruction within the Trustee.
> 3.3 **Use or Disclosure of Personal Health Information is acceptable only as part of one's job duties and responsibilities** (including reporting duties imposed by legislation) and **based on the need to know**.
> 3.5 **Employees and Persons Associated with the WRHA/Health Care Facility shall attend a WRHA PHIA Orientation and sign a WRHA Pledge of Confidentiality as a condition of employment/ contract/ association/ appointment.** The pledge must be signed as soon as reasonably practicable, but not later than three (3) months after commencement of their relationship with the WRHA/Health Care Facility.
> 3.7 The WRHA Pledge of Confidentiality shall be signed each time there is a substantial change in an Individual's position, as determined by the department, program or division responsible for the person, (i.e. an employee moves from a department with little exposure to Personal Health Information to a department that collects or maintains large amounts of Personal Health Information).
> 3.8 Employees and Persons Associated with the Trustee may be required to attend an additional PHIA Orientation and sign another WRHA Pledge of Confidentiality, at the discretion of the Privacy Officer, (i.e. disciplinary purpose).

The Confidentiality Pledge

WRHA employees are asked to sign a confidentiality pledge which is required by its "Confidentiality of Personal Health Information Policy" and section 7 of the regulation. The "Trustees Guide to The Pledge of Confidentiality" developed by Manitoba Health states that, "the Pledge of Confidentiality is above all an acknowledgement of *internal* security policies and

procedures for maintaining the confidentiality of personal health information." By signing a confidentiality pledge the WRHA employee acknowledges the following:

- That they have been made aware of WRHA policies "on use, collection, disclosure, security, storage and destruction of personal health information."
- That they have been "informed of the contents of the WRHA's Personal Health Information Confidentiality Policy and the consequences of a breach of personal health information."
- That they understand that "unauthorized use or disclosure of such information may result in a disciplinary action up to and including termination of employment/contract/association/appointment, the imposition of fines pursuant to The Personal Health Information Act and a report to my professional regulatory body."
- That they agree, as an integral part of the terms and conditions of their employment with the WRHA or a health care facility within the WRHA, that they will not at any time during or after employment disclose any personal health information "except as may be required in the course of [employment] duties and responsibilities and in accordance with applicable legislation and corporate policies governing proper release of information."

In this case, the HSC employee had signed a confidentiality pledge approximately one month (Feb 2012) before accessing the complainant's PCR record in apparent clear disregard of the confidentiality pledge.

Orientation to Internal Policies and Procedures

Under section 6 of the PHIA regulation the trustee is required to provide orientation to the internal policies and procures of their organization. As part of our investigation, we requested that the WRHA provide information about their orientation and training activities with regard to their PHIA policies and procedures. Employees such as the one in this case are required to undergo periodic training in the application of PHIA in their workplace. The HSC provided our office with a copy of their "Privacy Refresher" presentation, normally conducted by the HSC privacy officer.

The presentation reviews the responsibilities of the WRHA (and its employees) under PHIA and discusses the concept of confidentiality. Sample scenarios illustrate the practical application of confidentiality concepts in the health care workplace and make clear what constitutes a breach of confidentiality. Possible sanctions for unauthorized use or disclosure are stated as "a disciplinary response" which may include an oral or written warning, suspension or termination of employment. The possibility of conviction of an offence under the act is also made clear.

In this instance the employee would have attended a PHIA awareness session in February of 2012, on the same day as signing her most recent confidentiality pledge. Previous to that, the

employee would have attended an awareness session sometime between 1997, when PHIA was proclaimed, and 2000. The PHIA regulation does not stipulate how often the pledge must be renewed. However, generally speaking a gap of twelve years in awareness programming is less frequently than might be considered ideal. The WRHA is moving towards the implementation of an online learning tool that will be used for PHIA awareness education for all WRHA staff with an email address. Completion will be tracked electronically. The WRHA aims to have the tool go live by December 2013. The WRHA is also considering other methods to improve PHIA education to all staff, including increasing the frequency for confidentiality pledge renewal to between two and five years.

Tracking User Activity

Even with all the measures implemented by the WRHA, it is difficult for the health information trustee to protect against a determined and ethically-challenged employee who is unmoved by training and awareness campaigns. Our investigation illustrates that, while the WRHA may have exemplary policies and procedures in place to safeguard the personal health information it controls, at the end of the day the WRHA must rely on its employees to obey policies and follow appropriate use protocols. When they do not, a procedure must be in place to uncover malfeasance.

Usually the only way to uncover a determined snooper is by tracking user activity through periodic audits of access to personal health information. Section 4 of the regulation sets out safeguards for records in electronic form and these include the ability to create and maintain a record of user activity (what information is accessed, when and by whom) and the requirement to conduct periodic audits of user activity to detect security breaches that might not otherwise come to the attention of the trustee.

The regulation requires that a record of user activity be maintained and audited in accordance with the *Guideline for Auditing Records of User Activity* set by the minister of health and approved on November 21, 2008. As explained in the guideline, records of user activity "support individual accountability for user access to personal health information" and identify potential weaknesses within an electronic information system. Subsection 4(3) of the PHIA subclause 4(3) of the regulation acknowledges that there are instances when a record of user activity is not required. However, generally speaking systems which contain anything more than basic demographic information ought to have an audit capability for tracking views as well as additions.

Audits may include tracking of access to health information outside of normal working hours, review of electronic transmissions of personal health information from the system to determine unauthorized use or disclosure, situations where the user has the same name, address or street name as the subject of the record, situations where information of VIPs is accessed, situations

where employees view other employees' records, where the record involves a highly sensitive diagnosis or a publically known event (i.e. child abuse), situations where staff from one department view records from another department or situations where remote access has taken place. Audits may also include access not corresponding to role (need to know), as in this instance. Good practice for an audit of a record of user activity includes conducting random versus focused audits.

In this case, the HSC privacy officer was able to request an "Audit of Access by User ID" of the PCR system. The dates and times the employee accessed the PCR and retrieved information about the complainant were compared to the actual dates and times of visits by the complainant to HSC. It was determined that the complainant had not actually visited HSC on the dates and times that access took place. Therefore, it could be determined that there would have been no reason for the employee to access this information in the course of her normal work related duties and the use of the complainant's personal health information was contrary to PHIA.

Other key issues and risks are to be assessed when determining the level of auditing and frequency of audits includes the ability of the system to audit. As previously noted, the WRHA explained to our office that the ADT system is a legacy system which existed prior to the proclamation of PHIA and which does not allow tracking by view only. The WRHA advised our office on April 15, 2013 that "as a result of this PHIA Breach, a request to enhance the audit capability of the Health Sciences Centre legacy ADT system especially ensuring 'view only' access is logged was submitted on March 4, 2013. The enhancement is currently being implemented along with enhanced audit capability for ease of use." A request for an update on the progress of this work on June 24, 2013 provided the information that that the work was never undertaken due to "an issue with disk storage and a personnel change." The chief privacy officer of the WRHA explained it was recently announced that HSC will be implementing the Regional ADT solution and "because of this no further enhancements will be performed on our aging system." The Regional ADT solution is expected to be implemented by the end of March 2014.

The complainant in this case was not advised that an audit of access to her personal health information on systems other than the ADT and PCR systems at HSC was conducted. This audit showed that there had been no other access to her personal health information. The complainant might have been reassured that there was no evidence of access to other systems. To proactively offer and provide audits in cases where an employee is found to have inappropriately accessed personal health information and violated patient privacy may go some way towards reassuring complainants.

Also, in this instance there was some evidence that the employee may have printed information from the complainant's health records on the ADT system. Any updated system should also have the ability to record when printing of records has taken place. The possibility of the existence of

paper copies is a continuing source of worry for the complainant in this case. To require the employee to sign an undertaking that no print outs were made and if there were any made, to undertake to return those print outs and any copies to the trustee, might be considered in future privacy breach investigations.

CONCLUSIONS

The ombudsman found that the WRHA employee's use of the complainant's personal health information was carried on outside the employee's work related duties and not authorized by section 21 of PHIA. Our office has therefore found that the complaint of use in a manner not authorized by *The Personal Health Information Act* is supported.

The ombudsman found that the WRHA employee's disclosure of the complainant's personal health information was carried on outside the employee's work related duties and not authorized by section 22 of PHIA. Our office has therefore found that the complaint of disclosure in a manner not authorized by *The Personal Health Information Act* is supported.

The investigation of the privacy breach and response by the WRHA was found to be appropriate in the circumstances. Our office has also found that, although areas of possible improvement have been noted, the Winnipeg Regional Health Authority has taken appropriate measures to protect the personal health information of the complainant as required by PHIA.

We wish to express our appreciation to the complainant for bringing this matter forward. We also wish to thank the complainant and the WRHA for their cooperation in completing this investigation.

August 28, 2013
Manitoba Ombudsman