Manitoba Ombudsman

REPORT WITH RECOMMENDATIONS ISSUED ON JULY 20, 2012

AND

RESPONSE TO THE RECOMMENDATIONS

UNDER

THE PERSONAL HEALTH INFORMATION ACT

CASES 2011-0513 AND 2011-0514

CANCERCARE MANITOBA

PRIVACY COMPLAINTS: USE OF PERSONAL HEALTH INFORMATION AND SECURITY OF PERSONAL HEALTH INFORMATION

PROVISIONS CONSIDERED: 18, 19, 20, 21, 39, 60, 63, 64 of *The Personal Health Information Act*; 2, 4, 5, 6, 7, 8 of the *Personal Health Information Regulation*; and Manitoba Health's Guideline for Auditing Records of User Activity

PUBLICLY RELEASED ON SEPTEMBER 12, 2012

SUMMARY OF REPORT WITH RECOMMENDATIONS AND RESPONSE

The Ombudsman received a complaint that an employee of CancerCare Manitoba had improperly accessed the personal health information of the complainant's daughter which was maintained in an electronic medical record. We investigated the extent of the privacy breach by the employee, who was not providing health services to the complainant's daughter and had no need to know the information for employment purposes. We also investigated the actions taken by the trustee to protect the personal health information. The Ombudsman made recommendations to CancerCare Manitoba to strengthen the protection of its patients' electronic personal health information.

CancerCare Manitoba accepted all of the recommendations. Under PHIA, a trustee has 15 days from the date of acceptance to comply with the recommendations. CancerCare requested additional time to comply with some of the recommendations. The Ombudsman agreed that the proposed time frames for implementation were reasonable.

Manitoba Ombudsman

REPORT WITH RECOMMENDATIONS UNDER

THE PERSONAL HEALTH INFORMATION ACT

CASES 2011-0513 AND 2011-0514

CANCERCARE MANITOBA

PRIVACY COMPLAINTS: USE OF PERSONAL HEALTH INFORMATION AND SECURITY OF PERSONAL HEALTH INFORMATION

PROVISIONS CONSIDERED: 18, 19, 20, 21, 39, 60, 63, 64 of *The Personal Health Information Act*; 2, 4, 5, 6, 7, 8 of the *Personal Health Information Regulation*; and Manitoba Health's Guideline for Auditing Records of User Activity

Note: The above provisions are referred to but not always quoted in this report. These provisions can be found at http://web2.gov.mb.ca/laws/statutes/ccsm/p033-5e.php

REPORT ISSUED ON July 20, 2012

SUMMARY: We received a complaint that an employee of CancerCare Manitoba had improperly accessed the personal health information of the complainant's daughter which was maintained in an electronic medical record. We investigated the extent of the privacy breach by the employee and the actions taken by the trustee to protect the personal health information. It was determined that the employee was not providing health services to the complainant's daughter and had no need to know the information for employment purposes. We also determined that the manner in which CancerCare Manitoba investigated and responded to the complaint about the privacy breach was inadequate in some respects.

The Ombudsman made both suggestions and recommendations to CancerCare Manitoba to strengthen the protection of its patients' electronic personal health information.

BACKGROUND

In October 2011 our office received two privacy complaints under *The Personal Health Information Act* (PHIA) against CancerCare Manitoba (CancerCare), a trustee under PHIA. The complainant requested that our office investigate the improper use of the personal health information of her daughter. She also asked that our office investigate whether her daughter's

personal health information had been protected by CancerCare in a secure manner as required by PHIA.

The complainant advised our office that she had suspected that an employee of CancerCare had accessed her daughter's health records without authority under PHIA. She informed us that her daughter, who is a minor, was not receiving the particular type of treatment that might require the employee's services.

The complainant advised our office that the employee is an acquaintance who lives nearby. She indicated that her family has a strained relationship with the employee. The complainant informed us that after her daughter was diagnosed with cancer in early April 2011, the employee had unsuccessfully tried to obtain information about her daughter from another person known to the complainant and the employee. The complainant indicated that the employee was told to leave her family alone by this other person.

The complainant suspected that after this attempt to obtain information failed, the employee abused her position at CancerCare and searched CancerCare's electronic medical record (EMR) for information about her daughter. She advised CancerCare of her belief that the employee improperly accessed this personal health information.

The complainant informed us that CancerCare had confirmed in writing on September 14, 2011 that the employee had breached privacy by accessing the personal health information of the complainant's daughter. CancerCare's letter included information respecting the date of the breach (recorded incorrectly as having occurred on April 23, 2011 when in actuality it occurred on April 13, 2011) and the name of the employee who had accessed, without authorization under PHIA, the EMR of the complainant's daughter.

The complainant informed our office that, at her request, CancerCare directed the employee not to have contact with her family when they are attending appointments at CancerCare. The complainant expressed concern to us that if she had not reported her suspicions to CancerCare, the privacy breach would not have been discovered. The complainant's family has been dealing with a life threatening illness and this privacy breach has resulted in significant additional stress on her family. In her letter of complaint, the complainant stated that "PHIA is a very integral part of providing assurances to patients and their families that only the necessary individuals are accessing private health information."

THE COMPLAINTS

Subsection 39(2) of PHIA provides individuals with a right of complaint to the Ombudsman about a breach of privacy.

The two complaints in question, that the trustee (its employee) had used personal health information contrary to PHIA and had failed to protect the personal health information in a secure manner as required by the Act, fall under clauses (a) and (b):

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.

The right of complaint may be exercised by the parent (or guardian) of a minor who does not have the capacity to make health care decisions. In this case, we determined that the parent of the minor child in question was authorized under clause 60(1)(e) of PHIA to file a complaint on behalf of her child.

INVESTIGATION

These two complaints arise from the unauthorized use of personal health information by an employee of a trustee. Situations where an employee accesses personal health information that the employee does not need to know for a work-related purpose are commonly referred to as "snooping". In snooping cases we must consider the actions of the employee as well as the actions and responsibilities of the trustee, CancerCare, within the context of the law and rules governing their actions.

As this complaint had already been reported to CancerCare and investigated by them, the focus of our investigation of the complaint under clause 39(2)(a) of PHIA, about the employee's unauthorized use of personal health information, was to determine the extent of the breach. This included ascertaining the details on when the patient's information had been accessed by the employee and the specific personal health information that was accessed.

Our investigation under clause 39(2)(b) of PHIA focused on whether the trustee, CancerCare, has protected personal health information in a secure manner as required under the Act.

Public confidence depends on a trustee's ability to safeguard personal health information and take privacy breaches seriously, particularly when the breaches are intentional. While most employees may adhere to the requirements of PHIA and the parameters set by the trustee, this cannot be taken for granted. Accordingly, the security of personal health information depends on a trustee's ability to prevent and detect unauthorized use of personal health information and to invoke consequences for employees who violate privacy requirements under PHIA.

As part of our investigation we reviewed policies and procedures relating to the security of personal health information in place at the time of the privacy violation, and the steps taken by CancerCare when the complainant informed them that she suspected her child's privacy had been violated. We also obtained written submissions from CancerCare and we had discussions with the complainant and CancerCare.

The following two sections detail our investigation of the two complaints.

EMPLOYEE'S USE OF PERSONAL HEALTH INFORMATION

Personal health information is defined under PHIA to mean recorded information relating to an identifiable individual's health, health care history or the provision of health care to the individual. The definition includes the Personal Health Identification Number (PHIN) and any other identifying number assigned to an individual, as well as any identifying information that is collected in the course of, and is incidental to, the provision of health care.

Accessing and viewing personal health information on an EMR constitutes a "use" under PHIA. Under subsection 20(1) of PHIA, a trustee is prohibited from using (and disclosing) personal health information except in the circumstances allowed under PHIA.

Additionally, a trustee has an obligation to limit the use of personal information by its employees, as follows:

> ***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.*

Section 21 of PHIA restricts a trustee's use of personal health information to only the purpose for which it was collected or received, unless otherwise authorized.

When a trustee's use of personal health information is not authorized (permitted) under section 21 of PHIA, as was the case with this complaint, the use constitutes a violation of privacy under the Act.

During our investigation into the extent of the employee's unauthorized use of the patient's personal health information, CancerCare advised our office that, in response to the complainant's concerns, it had conducted an audit of the EMR to determine whether the employee in question had accessed the patient's EMR. CancerCare reviewed the patient access log that shows which employees accessed the patient's EMR, the personal health information that was accessed and when it was accessed. The patient's EMR was created on April 13, 2011, and the patient access log verified that the employee in question had accessed the patient's EMR later that day.

We obtained a copy of the patient access log. From our review of the log and our discussions with CancerCare we determined that on April 13, 2011 the employee accessed the patient's EMR and opened the tabs (or fields) for patient notes, patient agenda and patient summary. The duration of time in which the patient's EMR was accessed by the employee totaled 2 minutes and 2 seconds. The employee opened three tabs to view the contents, which indicates that the information was not accessed accidentally.

As the child's EMR had just been created, little information was available at that time and in fact, the employee viewed only the child's name and cancer registry number in the EMR. This information falls within the definition of personal health information under PHIA as it relates to

the individual's health and the provision of health care to her by CancerCare. Additionally, the cancer registry number is an identifying number assigned to the child.

Shortly after April 13, 2011, when the employee accessed these tabs, additional information was entered into the child's EMR. This included medication information, diagnosis, notes and blood work results. Our review confirmed that, even though the breach was not identified until September 2011, the employee did not access the child's EMR again after April 13, 2011 and therefore did not view this information.

At the time of her complaint to our office the complainant had been unaware that she was entitled to receive a copy of her child's patient access log. Concurrent with issuing this report, our office is providing the complainant with a copy of the access log for the period April 1, 2011 to October 26, 2011 to show the activity on the patient's health records during that time, confirming that the employee accessed the record only once.

CancerCare advised our office that disciplinary action had been taken against the employee and that since the breach, quarterly patient access logs about this patient would be retrieved and reviewed for a period of one year. CancerCare also advised that the breach served as a reminder to provide more regular PHIA training to longer-term employees.

Our investigation confirmed that the employee's use of personal health information contravened the trustee's obligations under subsection 20(1) of PHIA and we determined the specific information that the employee accessed deliberately and without authorization under PHIA.

CANCERCARE'S SECURITY SAFEGUARDS

In terms of safeguarding personal health information, section 18 of PHIA requires that a trustee adopt reasonable safeguards to ensure the confidentiality and security of the personal health information. A trustee is required to take into account the degree of sensitivity of the information to be protected, as per section 19 of the Act. Personal health information about health care relating to cancer would be considered to be extremely sensitive.

Our investigation of whether CancerCare, as the trustee, has protected the personal health information in a secure manner as required by PHIA, reviewed CancerCare's compliance with the requirements under the Act and its handling of this privacy breach.

Risks to the privacy, security and integrity of personal health information come in a variety of forms, from inadvertent human error to failure of power sources needed to operate a building alarm system or electronic medical record program. Risk also arises due to curiosity or personal (non-professional) interest on the part of people working in the healthcare system. Because of this, the security safeguards required under PHIA and its Regulation are multi-faceted, and involve taking administrative, technical and physical measures to protect personal health information.

Physical measures to safeguard personal health information can include activities as basic as filing hard-copy records of personal health information in locked cabinets in a locked filing

room, or limiting access to a fax machine that transmits records of personal health information. Administrative measures to safeguard personal health information include establishing and complying with written policies and procedures that provide for the security of personal health information throughout its lifecycle, from the time it is collected to the time it is destroyed. Written policies and procedures are also required to provide for the recording of security breaches and establishing corrective procedures for responding to breaches.

Section 2 of *The Personal Health Information Regulation* under PHIA (the Regulation) sets out the following requirements for the contents of security policies and procedures:

> ***Written security policy and procedures***
> ***2*** *A trustee shall establish and comply with a written policy and procedures containing the following:*
> *(a) provisions for the security of personal health information during its collection, use, disclosure, storage, and destruction…*
> *(b) provisions for the recording of security breaches;*
> *(c) corrective procedures to address security breaches.*

The Regulation also requires a trustee to conduct orientation and ongoing training about its security policies and procedures for its employees and agents. The trustee must ensure that employees and agents sign a Pledge of Confidentiality, to acknowledge being bound by the policies and procedures and to acknowledge awareness of the consequences of breaching them.

Section 5 of the Regulation requires a trustee to determine the personal health information that each of its employees or agents will be authorized to access. A trustee is also required to implement controls to ensure that the personal health information is used only by authorized employees whose identity is verified and used for a purpose authorized under PHIA.

As set out in section 4 of the Regulation, personal health information in electronic form is subject to additional safeguards, reflecting the fact that this format often makes the information available to a wider audience than information in paper records. The Regulation includes a requirement for a trustee to maintain a record of user activity that documents what personal health information has been viewed and/or edited, when this took place and the employee(s) of the trustee that viewed or edited the personal health information. A record of user activity is both a technical and an administrative measure for safeguarding personal health information. For this measure to be truly effective, the trustee must engage in regular and robust auditing of user activities and employees and agents must be aware of the trustee's commitment to implementing this measure. The Regulation requires that the record of user activity is to be maintained and audited in accordance with guidelines set by the Minister of Health, a copy of which forms Attachment 1 to this report.

To ensure that all of a trustee's security safeguards remain effective in maintaining the security of personal health information, section 8 of the Regulation requires trustees to conduct regular audits of all aspects of its security safeguards, at least every two years, and to take appropriate and timely steps to remedy any deficiencies in its safeguards.

In view of the above-noted requirements of the Act, Regulation and Guideline, we reviewed documentation provided by CancerCare concerning its policies and procedures, training, pledge of confidentiality and audits of security safeguards.

SECURITY POLICIES AND PROCEDURES

CancerCare advised that in early 2011, prior to the discovery of the breach, it had started a comprehensive review of its PHIA-related policies and procedures to incorporate revisions for consistency with the privacy policies of other trustees and to more fully address the requirements of the legislation. This review is ongoing.

CancerCare provided our office with a copy of the documents referred to under section 2 of the Regulation. Specifically, we received a copy of the revised procedures entitled, "Security and Storage of Personal Health Information" (Security Procedure), "Reporting of Security Breaches related to Personal Health Information and the Corrective Procedures to be Followed" (Breach Procedure), and "Confidentiality of Personal Health Information" (Confidentiality Procedure).

After further discussion with CancerCare, we were provided with a copy of two procedures that were in effect at the time of the breach: "Security of Personal Health Information" and "Confidentiality and Personal Health Information".

Our comments about the policies and procedures that we reviewed are contained under the following sections.

Confidentiality Procedure

We reviewed the Confidentiality Procedure in effect at the time of the breach and the revised procedure. We observed that the current Procedure begins with a purpose statement to ensure that employees and agents are aware of the vital importance of privacy and confidentiality to the provision of quality healthcare, and to highlight the need to protect personal health information, throughout its lifecycle, in accordance with PHIA, *The Mental Health Act*, and other relevant legislation. In our view, this provides additional guidance and direction to help employees place their obligations under PHIA in the context of patient care.

We observed that the current Confidentiality Procedure has changed in another respect, in that it now states that *unauthorized use or disclosure of personal health information **may*** [emphasis added] *result in a disciplinary response up to and including termination of employment, contract, association, or appointment.* The Procedure previously stated that *unauthorized use or disclosure of personal health information **shall*** [emphasis added] *result in a disciplinary response….*

We acknowledge that a privacy breach may occur due to human error, rather than resulting from deliberate, wilful actions of an employee, and that a trustee would need to have discretion to determine the nature of disciplinary action in relation to the specific circumstances of a breach. However, the way the policy is currently worded could very well be seen to suggest to employees that they may not be subject to any disciplinary action as a result of wilful unauthorized breaches of patient privacy. In this regard, we make the following suggestions:

Suggestion 1: It may be instructive to employees if the wording in the Confidentiality Procedure makes a distinction between the disciplinary action that may arise from wilful versus unintentional breaches of privacy.

Suggestion 2: To ensure that employees understand the consequences of breaching CancerCare's policies and procedures, it is important that any changes to the wording of the Confidentiality Procedure in this regard be reflected in the Pledge of Confidentiality.

Security Procedure

The Security Procedure sets out the steps to be followed when a breach of security occurs. Within the document, a breach of security is defined as occurring whenever personal health information is collected, used, disclosed or accessed other than as authorized, or its integrity is compromised. We note that this definition would also describe a breach of privacy.

In our review of the Security Procedure, we observed that it does not include wording similar to that found in the Confidentiality Procedure that *all persons who become aware of a possible Breach of Security or Confidentiality of Personal Health Information shall refer to the 'Reporting of Security Breaches Related to Personal Health Information Policy'.* To ensure that employees understand the trustee's expectations, we make the following suggestion:

Suggestion 3: It may provide greater clarity to include wording respecting the reporting of a breach, similar to that found in the Confidentiality Procedure.

Breach Procedure

The Breach Procedure speaks to the necessity for reporting, recording and analyzing all breaches of the confidentiality and integrity of personal health information. It identifies corrective procedures for remedying breaches, and requires that these procedures be followed. Where the breach is as a result of an alleged violation on the part of an employee, it is to be investigated with involvement of the Privacy Officer, Human Resources, and the alleged violator's Supervisor. Among other things, the investigation is to involve consideration of the description of events provided not only by the affected individual but also by the employee alleged to have breached the individual's privacy.

Our comments arising from our review of the trustee's investigation of this privacy breach are contained under the heading Comments and Suggestions about CancerCare's Investigation of the Privacy Breach, on page 13.

PHIA TRAINING REQUIREMENTS

Section 6 of the Regulation speaks to the requirement for the trustee to provide orientation and ongoing training to staff about the trustee's policies and procedures. CancerCare advised that its PHIA orientation is mandatory and that all new employees normally receive PHIA and Confidentiality orientation and training within their first week of employment or shortly thereafter. We asked the trustee to describe in more detail the PHIA training it provides to staff. CancerCare advised that it offers a new employee corporate orientation, normally scheduled on a

quarterly basis, at which time PHIA obligations are reviewed. When space permits, Directors, Managers and Supervisors are encouraged to send their longer term employees for training to promote ongoing learning and awareness of employee obligations. CancerCare also indicated that all employees are notified by the Corporate Policy Committee when policies are updated. Additionally, the CancerCare Privacy Office offers privacy tools to all staff on its Corporate Shared Drive - Privacy Folder. A Power Point presentation and video are also available to all staff. The video is entitled, "The Personal Health Information Act and Understanding your Role". Furthermore, PHIA tips are shared via email to all staff.

CancerCare acknowledged the importance of ongoing education in relation to its policies and procedures and employee obligations under PHIA and felt this responsibility could be managed by CancerCare Departmental Directors, Managers and Supervisors, during regular staff meetings. Confidentiality and PHIA are among the topics discussed at these meetings, and the meetings provide a forum to review and discuss any learning opportunities that arise, such as the privacy breach that is the subject of this report.

While CancerCare does provide orientation and ongoing training to its employees about its policies and procedures, we understand that it does not track employees' participation in ongoing training. We are of the view that tracking employees' participation is essential to ensure that all employees, including longer term employees, are regularly reminded of their obligations respecting privacy, and are aware of any amendments to PHIA or the Regulation and any changes to the trustee's policies and procedures.

PLEDGE OF CONFIDENTIALITY

Section 7 of the Regulation states that trustees are to ensure that each employee signs a pledge of confidentiality that includes an acknowledgement that he or she is bound by the policy and procedures referred to in section 2 of the Regulation and is aware of the consequences of breaching them.

We reviewed two pledges of confidentiality signed by the employee in question. The first pledge was dated in 2002. After the privacy breach, CancerCare required the employee to attend a one-on-one PHIA reorientation with the Privacy Officer, following which the employee signed an additional pledge. The wording of the pledges is identical and both include the statement:

> *I also understand that unauthorized use or disclosure of such information will 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.*

We were advised by CancerCare that the employee group to which the employee belongs does not have a regulatory body.

CancerCare also provided our office with a copy of another pledge that we understand is under consideration. It differs somewhat from the current version in that it includes, in addition to what was previously noted respecting the policy and procedures, that the individual has attended an

orientation regarding PHIA. Additionally, the wording with respect to disciplinary action has been changed from …*unauthorized use or disclosure of such information* ***will*** [emphasis added] *result in a disciplinary action*… to …*unauthorized use or disclosure* ***may*** [emphasis added] *result in a disciplinary action....*

CancerCare advised that it works in partnership with other trustees in Manitoba and indicated that other trustees have used the word "may" on their pledges of confidentiality. CancerCare indicated that adopting this pledge would maintain standardization and consistency with other trustees.

We note that the proposed revision to the pledge would also reflect the revised wording in the Confidentiality Procedure, about which we expressed concern earlier in this report. Our comments there apply equally here and, in that regard, we make the following suggestion:

> Suggestion 4: It would be instructive to employees to make a distinction between wilful and unintentional unauthorized uses or disclosures under PHIA and the resulting disciplinary action. In this regard, it would seem reasonable for a trustee to exercise discretion for discipline for unintentional unauthorized uses or disclosures, depending on the circumstances. However, for wilful breaches of privacy, it would be appropriate for a trustee to make it clear to an employee that such actions are not acceptable, by stating that this *will* result in a disciplinary action and that it *will* result in a report to a professional regulatory body, if the employee is a regulated health professional. It may also be prudent to create a policy that sets out the progressive discipline regime respecting unauthorized and wilful uses or disclosures.

CancerCare advised that it has a progressive discipline regime in place. We reviewed CancerCare's disciplinary action towards the employee who had used the personal health information of the complainant's daughter in contravention of PHIA. Documentation of the PHIA breach was included in the employee's personnel file, and the employee received a warning letter about the seriousness of the breach, and a direction to govern herself in accordance with PHIA. The employee was required to attend a meeting with both the Chief Human Resources Officer and the employee's Program Director to review the breach, during which the employee expressed remorse and regret, and committed that she would not violate PHIA again. The employee also signed a document indicating that any future breach of PHIA would result in more significant disciplinary action, such as termination of employment.

ACCESS PRIVILEGES, TRACKING USER ACTIVITY AND AUDITS

Access

Ensuring the protection of personal health information in electronic form requires that a trustee limit access to employees who need to know the information, track employees' access to the information and conduct regular audits to detect and address any breaches by employees.
To determine compliance with subsection 20(3) of PHIA, we asked CancerCare to explain the process for determining its employees' access privileges to the electronic personal heath information. CancerCare advised us of the following:

> *Care provider access to patients' charts is currently set up on an INSTITUTION basis. The care provider can access any patient record within the specific institution.*

What this means is that all employees at a particular CancerCare site have the ability to access the personal health information of all patients who are provided with care at that site. For example, all employees at the MacCharles site had access to information about the complainant's daughter, whether or not they were providing her with care.

The employee in question works in an area of the site that provides a health service that did not form part of the complainant's daughter's treatment program. Therefore, as it did not appear to be necessary for any employee in this area to have access privileges to the complainant's daughter's personal health information, we inquired with CancerCare about the ability to further limit access to personal health information within each institution. CancerCare advised that:

> *ARIA, our EMR solution at CancerCare Manitoba does have the ability to grant access and privileges in the application according to role and access can also be granted site based.*
>
> *The Director, Manager, and Supervisor upon hire of a new employee or change in position or role submits a Request for Service to CancerCare's Information Services Department. The computer account and access is set up according to the employee's role, position and area of responsibility.*
>
> *CancerCare Manitoba's Information Services Department has identified the need to establish a regular review process of user access privileges and advises this will be undertaken shortly and adopted as an annual process.*

We acknowledge the logistical difficulties in implementing a system where access privileges for each employee are defined in relation to each patient, one-at-a-time, as such a system may not always provide a trustee with sufficient flexibility to respond to changes in a patient's condition or treatment, or to deliver care in an emergency. However, we did ask CancerCare to explore whether it was feasible to further limit access privileges within each site. CancerCare recently confirmed with our office in May 2012 that a project to restrict access has been started as a result of determining the system is capable of restricting access to individual employees and by role as well as institution. The project outline provided for our review identifies multiple steps in this project and CancerCare anticipates the project will be completed by June 2013.

Furthermore, CancerCare advised our office that, effective May 31, 2012 the employee in question, and all employees from that particular health service area, were blocked from accessing the patient's file. CancerCare had earlier committed to monitoring the child's patient access log until the time that the blocking feature was enabled, and confirmed that the employee did not enter the child's file again.

Tracking

With respect to tracking user activity, CancerCare's patient access log tracks users of the system. The log produces the following information:

- Patient Name
- CancerCare employee username
- Windows that were accessed within ARIA (CancerCare's electronic health system)
- Date/time the information was accessed
- Total time that the record was accessed

The log we reviewed in relation to this complaint does not indicate whether any information has been printed from the EMR. We asked CancerCare to clarify the capabilities of the system. CancerCare advised:

> *Certain modules within its system, ARIA, do log users printing ARIA information. CancerCare Manitoba is investigating which modules offer this audit trail. Windows and other products such as (SnagIT) allow users to do screen scrapes, which allow any user to print off any screen within ARIA. Audits do not exist for this type of activity.*

The ability to ascertain whether personal health information has been printed enables better tracking of the information. Knowing whether the information has been printed could assist in determining if there has been a disclosure and assessing risks relating to such a disclosure. For example, if an employee has inappropriately accessed the personal health information of a patient, it would be of use to know whether the employee also printed the information. Efforts could then be made to identify the use made of the printed information to determine if it had been shared with others, and to recover it.

> Suggestion 5: If an unauthorized use has occurred, and printing cannot be tracked, the employee should be required to sign a statement indicating whether the information was printed and/or disseminated, and if so, details should be included to explain what the employee has done with the information.

Audits

The auditing of user activity with respect to electronic personal health information is critical in order to detect and address breaches due to employees' unauthorized use of personal health information. Periodic auditing of all of a trustee's security safeguards ensures that changing risks in the environment are identified and accounted for and that the security safeguards remain relevant and effective.

We asked CancerCare about its auditing of the security safeguards it has in place to protect personal health information. CancerCare advised that it had conducted a Privacy Compliance Audit of forty-five of its departments during February and March 2011 to determine its level of compliance with respect to security safeguards.

Our office reviewed the Privacy Compliance Audit and found that although it demonstrated a high level of compliance with the measured safeguards, it was structured to measure mainly administrative and physical security safeguards, and did not look at technical safeguards specifically relating to electronic personal health information.

We asked CancerCare about its auditing of its EMR system. We were advised that detailed Patient Access Logs are readily available for review to assist in the investigation of security breaches. In addition, CancerCare is participating in an audit of its employees' access to the electronic record system of another trustee. This audit is specifically aimed at "same name" searches by employees and would help to identify possible incidents of employees accessing personal health information of family members. While we recognize these positive efforts, we are of the view that the Minister's Guideline contemplates a more comprehensive approach to auditing user activity, one that encompasses routine audits as well as audits focused on specific types of scenarios in which an unauthorized use is likely to arise.

CancerCare advised that the Provincial and Regional Privacy Officers are collectively reviewing electronic auditing and reporting criteria. We understand from Manitoba Health that the Provincial and Regional Privacy Officers are being consulted as part of the process of reviewing and potentially revising the Minister's Guideline for auditing records of user activity. Best practices identified by ongoing research at the national level may also be reflected in revisions to the guidelines.

Regular audits of user activity are critical, in our view, for ensuring that the use of electronic personal health information is compliant with PHIA and detecting any breaches by employees.

COMMENTS AND SUGGESTIONS ABOUT CANCERCARE'S INVESTIGATION OF THE PRIVACY BREACH

We note that in this case, the breach was suspected by the complainant, who reported it to CancerCare. CancerCare investigated and confirmed the breach by the employee. The complainant advised our office that she had spoken with three CancerCare employees about the breach. The complainant indicated to us that she had lingering questions about the breach that were not answered, including what was the specific personal health information viewed by the employee, whether it could be determined definitively that the employee had only accessed the child's EMR once, and what reasons the employee gave for having accessed the information.

The complainant indicated that CancerCare did not initially advise her of the right to request a copy of the patient access log, which indicates the employees who accessed her child's EMR and the specific personal health information contained in the EMR. Had CancerCare provided the log to the complainant, the first two questions would have been answered. It would be a good practice for a trustee to proactively offer and provide the patient access log when an employee has inappropriately accessed the EMR and violated patient privacy.

The complainant advised our office that CancerCare did not provide an answer to her question about the employee's reason for choosing to access the EMR of her daughter. The complainant

informed us that CancerCare had told her that they had to protect the employee's privacy and would not reveal this information unless the employee allowed them to do so.

We note that if an employee does not need to know the personal health information to carry out their job duties, this would be an unauthorized use regardless of the reason for accessing the information. However, in our view, the reason for accessing the information would be an important consideration in a trustee's investigation and potential corrective measures to be taken, including disciplinary action. The veracity of an employee's stated purpose or reason for deliberately entering the record of a patient to whom they are not providing health care should be tested through sharing that information with the patient (or their representative), especially when a personal relationship between the employee and the patient appears to have been a factor in the employee's actions.

With regard to CancerCare's procedures for investigating privacy breaches, we suggest that CancerCare incorporate the following into the investigation procedures:

1) Proactively offer to provide the complainant with a print-out of the access log
2) Test the veracity of the employee's reason for accessing the patient record, through interviews with the employee and the complainant.

Additionally, if a privacy breach is substantiated, the trustee should incorporate the following procedures:

3) Require the employee to sign an undertaking confirming that the employee did not copy or print any of the patient's personal health information and that the employee has not and will not disclose any of the information
4) Provide the complainant with an explanation of the penalty imposed on the employee for the violation of privacy, including any disciplinary action taken
5) Inform the complainant of the right to complain to the Ombudsman about the breach

OBSERVATIONS ABOUT SANCTIONS FOR PRIVACY BREACHES

The preamble of PHIA recognizes the sensitivity of health information and the need to protect confidentiality of it so that Manitobans are not afraid to seek health care or provide sensitive information that may be necessary to facilitate their care. The preamble also recognizes that rules to protect personal health information are an essential support for electronic health information systems.

PHIA has been in effect in Manitoba since 1997. As stated in the preamble to PHIA, privacy concerns may influence patients seeking health care and this has been recently demonstrated in a survey of Canadian patients' beliefs about care providers' responsibility to protect patient privacy, published in December 2011. The survey, *Canada: How Privacy Considerations Drive Patient Decisions and Impact Patient Care Outcomes* is available online at www.fairwarning.com/documents/Canada/2011-CanadaSurvey.pdf.

Some of the key findings of the survey are:

- Trust in the confidentiality of medical records is influencing when, where, who and what kind of medical treatment is delivered to Canadian patients. Canadian patients demonstrate that privacy concerns impact how quickly they seek care, the medical information they share with their provider, and from whom they seek care. These privacy concerns affect how Canadian providers can diagnose medical conditions and deliver appropriate care.
- Canadian patients expect healthcare providers and hospital executives to aggressively protect patient privacy. Patients have a significant negative response when privacy violations occur and expect healthcare executives to be held accountable for breaches.
- Canadian patients have a strong belief that additional privacy laws and greater enforcement of privacy laws would provide a greater impetus for healthcare providers to take privacy more seriously.

In this case the employee violated the privacy protections afforded to Manitobans under PHIA, by snooping in the electronic health record of another person. However, this violation of privacy is not considered to be an offence under subsection 63(2) of PHIA, as only a wilful unauthorized disclosure is considered an offence. A conviction on such an offence can result in a fine of up to $50,000.00.

The use of personal health information, in this case snooping in a patient's electronic health record, is not an offence in Manitoba.

This differential treatment of violations of privacy, use versus disclosure, by an employee, has the potential to enable a lack of accountability for an employee's deliberate unauthorized use.

We note that other sanctions may be available if the employee is a regulated health professional governed by a regulatory body. The conduct of the employee can be referred to the regulatory body, which may apply sanctions such as issuing reprimands or revoking a licence. In this particular case, the employee in question was not a regulated health professional.

Although Manitoba was the first province in Canada to enact privacy legislation specific to personal health information, six other provinces now have health information privacy legislation in force: Alberta, British Columbia, New Brunswick, Newfoundland/Labrador, Ontario and Saskatchewan. Five of these six statutes contain offence provisions for unauthorized use of personal health information by a "person" (rather than limiting the offence to solely a "trustee"). The health privacy legislation in other provinces providing for sanctions against an employee who inappropriately accesses personal health information, offers a model for amendments to strengthen PHIA.

Snooping in electronic health records is an evolving privacy issue. There have been some publicized cases in other provinces where significant sanctions, including prosecutions under health privacy legislation and fines, have been levied against the offending employee. We have included some examples of sanctions in other provinces, in Attachment 2.

In paper-based records systems, snooping is restricted by virtue of employees needing to be in the same location as the paper file. Electronic systems for maintaining personal health information increase the risk of a privacy violation occurring through snooping because significant amounts of information about thousands of individuals is readily accessible through a few computer keystrokes by an employee. It is important that privacy breaches by employees are taken seriously by trustees in order to inspire public confidence. As indicated in the key findings in the above-referenced privacy survey of patients, public confidence is also enhanced by strong privacy laws that are enforced.

In light of our observation about the lack of offence penalty under PHIA for wilful unauthorized use by an employee, and our comparison with other provinces, we have brought this issue to the attention of Manitoba Health.

RECOMMENDATIONS

The Ombudsman has made the following recommendations to CancerCare to ensure the protection of its electronic personal health information and to foster Manitobans' confidence in the privacy of their personal health information:

1. **The Ombudsman recommends that CancerCare send a letter to the complainant, apologizing for the employee's breach of privacy.**

2. **The Ombudsman recommends, in accordance with section 6 of the Regulation, that CancerCare conduct ongoing PHIA training for all staff and that such training be tracked by CancerCare.**

3. **The Ombudsman recommends, in accordance with subsection 8(1) of the Regulation, that CancerCare conduct an audit of its security safeguards every two years, including administrative, technical and physical safeguards.**

4. **The Ombudsman recommends that CancerCare investigate which modules within its ARIA system offer an audit trail when personal health information is printed and provide the findings to our office.**

5. **The Ombudsman recommends that CancerCare ensure its security practices adhere to the Guideline for Auditing Records of User Activity.**

6. **The Ombudsman recommends that CancerCare, further to developing a formalized plan for auditing its electronic personal health information, provide our office with a report on its plan on how it will detect unauthorized use and disclosure of personal health information.**

7. **The Ombudsman recommends that, when investigating and responding to any future privacy breach of this kind, CancerCare proactively communicate with the affected individual to ensure the individual knows the specific personal health information that was breached, when and why it was breached, and the steps that CancerCare has taken and will be taking to protect the individual's privacy in the wake of the breach.**

TRUSTEE'S RESPONSE TO THE RECOMMENDATIONS

Under subsection 48(4) of the Act, the trustee must respond to the Ombudsman's report in writing within 14 days of receiving this report. As this report is being sent by courier to the trustee on this date, the trustee shall respond by August 3, 2012. The trustee's response must contain the following information:

> ***Trustee's response to the report***
> ***48(4)*** *If the report contains recommendations, the trustee shall, within 14 days after receiving it, send the Ombudsman a written response indicating*
> *(a) that the trustee accepts the recommendations and describing any action the trustee has taken or proposes to take to implement them; or*
> *(b) the reasons why the trustee refuses to take action to implement the recommendations.*

TRUSTEE'S COMPLIANCE WITH RECOMMENDATIONS

If the trustee accepts the recommendations, subsection 48(6) of the Act requires the trustee to comply with the recommendations within 15 days of acceptance of the recommendations or within an additional period if the Ombudsman considers it to be reasonable. Accordingly, the trustee should provide written notice to the Ombudsman and information to demonstrate that the trustee has complied with the recommendations and has done so within the specified time period.

Alternatively, if the trustee believes that an additional period of time is required to comply with the recommendations, the trustee's response to the Ombudsman under subsection 48(4) of the Act must include a request that the Ombudsman consider an additional period of time for compliance with the recommendations. A request for additional time must include the number of days being requested and the reasons why the additional time is needed.

Subsection 48(7) of the Act provides that the Ombudsman must make recommendations made under this section available to the public, and may do so by publishing them on a website.

July 20, 2012
Mel Holley
Acting Manitoba Ombudsman

ATTACHMENT 1

GUIDELINE

Auditing Records of User Activity

Approved by Arlene Wilgosh, Deputy Minister of Health and Healthy Living on November 21, 2008.

LEGISLATIVE REFERENCE

The Personal Health Information Regulation (the "regulations") states:

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

4(2) A record of user activity may be generated manually or electronically.

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

DEFINITIONS

Access refers to the ability to view (read), add to (write), modify (amend/update/merge), delete and/or transmit (email/fax/print) information contained within an electronic information system.

Auditable Event means the type of information within an electronic information system or a component or module of an electronic information system that may be audited and includes but is not limited to: demographic/eligibility information, transmissions, security administration (see Appendix A).

Focused Audit is an audit of specific user activity or event based on the need to investigate unauthorized access or other security issues.

Level of Activity describes to what level a record of user activity will be created/maintained based on a trustee's review of key issues/risks and type of auditable event (information).

Random Audit is an audit of user activity or event for randomly selected timeframes.

Transmission refers to a specific action or process defined by a user such as faxing, emailing or printing. A trustee determines where a transmission is use or disclosure. This does not include system-to-system transmission such as data being transmitted without user intervention (see clause 4(3)(b) of the regulation).

User Access Role refers to the functionality assigned to a specific user or group of users who require access to personal health information maintained in an electronic information system to do their job. (e.g. read/view, add, modify, delete)

GUIDELINES

A record of user activity is created and maintained for the purpose of tracking and recreating relevant system events and actions. These records support individual accountability for user access to personal health information, identify potential weaknesses and assess security within an electronic information system.
In accordance with subsection 4(4) of the regulation a Trustee will establish a process for auditing records of user activity based on the following guidelines:

1. A trustee must review subsection 4(3) of the regulation to determine whether a record of user activity is required.

2. A trustee must designate one or more person(s) who will be responsible for creating and viewing the records of user activity.

3. A record of user activity is created based on the level of auditing (see definition) required for an electronic health information system (see Table 1).

4. The following are key issues/risks that should be assessed to determine the level[1] of auditing and the frequency of audits when creating a record of user activity of each electronic information system.
    - Type of auditable event within an electronic system (see Appendix A).
    - System ability to audit
    - Scope of system
        - Size and complexity
        - Number of users (i.e. multiple or one or two)
        - Type, sensitivity and amount of information within a system
        - Inter-departmental/facility
        - Cross jurisdictional, cross border systems
    - Required professional standards and business/legal requirements
    - Outsourcing and third party access
    - Probability of potential risk

5. The frequency of auditing will be established based on the key issues/risks identified (4 above) in the electronic health information system.

6. An audit of records of user activity includes, but is not limited to:
    - Conducting random versus focused audits,
    - Determining reasonable/attainable numbers of records for review as part of a random audit,
    - Determining reasonable/attainable frequency of record audits,
    - Establishing a rotation for routine audits (i.e. varying day/week/month/time of day)

7. Audits may include the following:
    - Access not corresponding to role of the user, "need-to-know".
    - Review of electronic transmission of personal health information from the system to determine unauthorized use or disclosure.
    - Access to health information systems outside user's normal working hours.

[1] NB - Development of a rating scale for these issues/risks to assist in creation of the audit requirements.

- Information accessed where:
  - User has the same last name, address or street name as the individual the information is about,
  - VIPs (board members, celebrities, government or community figures, physicians, management staff or other highly publicized individuals),
  - Employees viewing other employee records,
  - Cases with a highly sensitive diagnosis (HIV, Psychiatric disorders) or publicized event (child abuse),
  - Staff from one department viewing records from another department,
  - All remote access.

8. A process is established for the occasional audit of security administrator records of activity (i.e. "check the checker")

9. Access to records of user activity must be limited to authorized staff only.

Table 1

The following table, in alignment with issues/risks identified in Guideline 4, may be used to assist trustees in determining an appropriate level of auditing required when creating a record of user activity. The following levels are suggested minimums based on the type of event.

	LEVEL OF AUDITING					
AUDITABLE EVENTS	**No Record of User Activity Required**	**Views (Read/Query)**	**Additions (Write)**	**Modifications (Amend/Update)**	**Deletions (Cancel)**	**Transmissions (Fax/Email)**
Demographic/Eligibility Information within a registry or other database where the use of the registry/database identifies personal health information about an individual (outside of PHIA, Schedule B)		×	×	×	×	×
Scheduling Data						
▪ Demographic, date and time information (may include provider/program)	×					
▪ Demographic, date and time and personal health information (i.e. type of surgery)		×	×			
Clinical Care Data						
Structured Data		×	×	×	×	×
Text Data		×	×	×	×	×
Document Image Data		×	×		×	×
Signal Tracing/Monitoring Data					×	×
Diagnostic Image Data		×	×		×	×
Video Data	×					
Audio Data	×					
Decision Support Tools[2]	×				×	
Non-Clinical Care Data (contains personal health information)						
Research		×				×
Peer Review		×				×
Audits		×				×
Financial (i.e. physician billing)		×				×
Report Generation						
Canned Reports		×				×
Ad Hoc Reports		×				×
Security Administration Data						
Record of User Activity		×	×	×	×	

[2] Will require additional discussion – i.e. new versions/updates

APPENDIX A

Auditable Events

1. **Scheduling Information:** Information collected within a scheduling system that may contain minimal demographic/eligibility information, date and time of scheduled encounter, provider/program and type of encounter (i.e. ultrasound).

2. **Clinical Care Information:** Clinical care information includes, but is not limited to the following:

Structured Data: Predefined and limited (i.e. dropdown lists)

- Orders (Lab, DI, Medication, Treatment, Referral)
- Medication Administration
- Online charting (Assessments, Protocols, Nursing History, Graphic Records, etc.)

Text Data: Transcribed information

- Transcribed Reports (Radiology, Pathology, History & Physical, Consultation, Surgical, etc.)
- Email
- Patient education information (i.e. Discharge instructions)

Document Image Data: Scanned documents

- Scanned written documentation (i.e. consents, correspondence, paper clinical care documentation)
- Digital photos

Signal Tracing/Monitoring Data:

- ECG/Hemodynamics
- EEG/Sleep Study
- Fetal Heart Tracing

Diagnostic Image Data:

- Computed radiography and tomography
- Magnetic Resonance Imaging
- Nuclear medicine scans
- Ultrasound images
- Pathology images

Video Data:

- Ultrasound
- Cardiac catheterization

Audio Data:

- Voice dictation and annotation

Decision Support Tools:

- Pop-ups, Alerts, Reminders

APPENDIX A

Auditable Events

3. **Non-Clinical Care Information:** (containing personal health information)
    - Research Data
    - Peer Review Data
    - Audits
    - Statistical
    - Financial

4. **Report Generated Information:**
    - Canned Reports
    - Ad Hoc Reports

5. **Security Administration Information:**
    - Records of User Activity
    - Created and Removed User Accounts
    - Assigned and Changed Privileges
    - Changes to Configuration

ATTACHMENT 2

EXAMPLES OF SANCTIONS FOR UNAUTHORIZED USE IN OTHER PROVINCES

Example 1

In Alberta, a medical records clerk wilfully and without authorization, accessed personal health information on the provincial electronic health system called Alberta Netcare. The health information pertained to the wife of a man with whom the clerk was having an affair. The wife was being treated for cancer. An investigation by the office of the Information and Privacy Commissioner of Alberta determined that the clerk accessed the personal health information on six different days.

The actions of the clerk constituted an offence under Alberta's *Health Information Act*. The clerk was prosecuted for this offence in 2007, which was the first prosecution of an offence under Alberta's Act. The clerk pleaded guilty and was fined $10,000.

Information about this matter can be found at
http://www.oipc.ab.ca/Content_Files/Files/News/NR_HIAchargeCourt_Apr_16_07.pdf

Example 2

Similarly, in another case in Alberta, a physician wilfully and without authorization, used personal health information on Alberta Netcare in 2010. The complainant suspected that his ex-spouse (a nurse) and/or her new partner (a physician), both of whom worked at a hospital, had accessed his personal health information in contravention of Alberta's *Health Information Act*. The complainant and his ex-spouse were involved in divorce proceedings at the time. He requested access to audit log reports to determine who had accessed his personal health information.

The complainant discovered that 12 physicians, who were not his care providers, were shown to have accessed his personal health information through Netcare. It was later discovered that it was the physician (the new partner of the complainant's ex-spouse) that had contravened the Act by accessing personal health information from computers that had been logged onto by these 12 physicians. The personal health information was accessed for personal reasons, i.e., to determine the complainant's medical history. The physician also improperly accessed the records of the complainant's new partner as well as the complainant's mother. The Information and Privacy Commissioner of Alberta determined that it was not feasible to pursue an offence because of a lack of admissible evidence.

This matter was also referred to the College of Physicians and Surgeons for investigation into the physician's conduct and the hospital issued the physician a letter of reprimand.

It was also found that the hospital had not taken reasonable measures to protect the personal health information. While the hospital had established a policy advising users to log out of applications when leaving a computer terminal unattended, there was no evidence to show that

the 12 physicians had been trained in how to use the system securely. Therefore, the 12 physicians were not found to have contravened the Act.

Additional information can be found at
http://www.oipc.ab.ca/downloads/documentloader.ashx?id=2912

Example 3

A pharmacist in Alberta accessed personal health information (prescription drug information) on Alberta Netcare of members of her church congregation. One of these members had complained to the church about the pharmacist's relationship with a male member of the congregation. The pharmacist then posted information on Facebook relating to prescription drugs being taken by the complainant and 8 other women who the pharmacist believed were sympathetic to the complainant. Following an investigation, the Information and Privacy Commissioner referred the matter to the Department of Justice for prosecution. This was the second prosecution under Alberta's *Health Information Act*. The pharmacist was charged with 11 counts of knowingly obtaining or attempting to obtain health information in contravention of the Alberta's *Health Information Act*. In 2011, she pleaded guilty to a single charge and was fined $15,000.

Additionally, the Alberta College of Pharmacists conducted an investigation into unprofessional conduct relating to this unauthorized access by the pharmacist. The sanctions imposed were as follows:

- Levied a fine of $4000 ($1000/individual)
- Suspended her practice permit for 4 months
- Ordered her to pay the costs of the hearing up to a maximum of $11,000
- Published the decision in the College's newsletter with her name
- Notified all pharmacist regulatory bodies in Canada
- Verbally reprimanded her at the hearing

Further information can be found at
http://www.oipc.ab.ca/Content_Files/Files/News/NR_Prosecution.pdf

Example 4

A pharmacist in Saskatchewan was found to have inappropriately viewed personal health information of a former friend and his family, who had previously been patients of the pharmacy. The pharmacist had been involved in a business arrangement with the man but this was dissolved and the professional patient-pharmacist relationship was severed. Subsequently, the pharmacist viewed on 9 different occasions the personal health information of this former long-term friend and two of his family members, through the Pharmaceutical Information Program (PIP), which is the centralized database of prescription records in the custody of Saskatchewan Health. This privacy breach was detected when the patient requested information on who had viewed his drug profiles and the profiles of his family members.

The Saskatchewan College of Pharmacists investigated this matter and determined that the viewing was not appropriate, however, it did not take any disciplinary action against the pharmacist.

The Information and Privacy Commissioner of Saskatchewan investigated this breach under that province's *Health Information Protection Act* (HIPA). The Commissioner made recommendations to address deficiencies in compliance with the requirements of the Act. The recommendations included developing policies and procedures to safeguard the personal health information, providing training to staff and ensuring that all staff sign a pledge of confidentiality.

More information can be found at http://www.oipc.sk.ca/Reports/H-2010-001,%20March%2023%202010.pdf

Example 5

In Ontario, a registered practical nurse in a hospital was found to have accessed personal health information of a patient to whom she was not providing health care services. The patient had alleged that during and after her stay in hospital in 2005, her personal health information was accessed by the nurse. The patient indicated that the nurse was her estranged husband's girlfriend. The patient's estranged husband also worked at the hospital. The patient and the estranged husband were involved in divorce proceedings and a custody battle for the children. Prior to and during her admission, the patient had alerted hospital staff of her concern about protecting her privacy given the circumstances. She also indicated that she had a restraining order against her estranged husband.

The estranged husband had phoned the patient after her discharge from hospital and made reference to a heart condition, which suggested that he had knowledge of her current treatment. Subsequently, the patient expressed her privacy concerns to the hospital. The hospital placed a "VIP flag" on the patient's electronic health record that alerts staff accessing her record that the patient's information was determined by the Chief Privacy Officer to be highly sensitive. An audit report would automatically be sent to the Chief Privacy Officer each time the patient's record was viewed. An audit on the electronic health record found that the nurse accessed the patient's file without justification. The hospital's investigation report to the patient referred to the nurse's unblemished 24 years of service and the estranged husband's good record throughout 21 years of service with the hospital. The report indicated that the nurse was suspended without pay for 4 weeks and the estranged husband for 10 days. The hospital had also issued a letter of reprimand to the nurse and to the husband.

The nurse had accessed the patient's information on ten occasions over a six week period during and after the patient's stay in hospital. This included three instances where the nurse disregarded electronic warnings about accessing the record after the VIP flag was initiated.

Further to receiving the hospital's report, the patient filed a complaint with the Ontario Information and Privacy Commissioner. The matter proceeded to adjudication and the review determined that the nurse's use of the personal health information was in contravention of Ontario's *Personal Health Information Protection Act*. The Commissioner found also that the

information was disclosed, in contravention of the Act, to the estranged husband. The Commissioner made an order to the hospital to review and revise its privacy procedures and to implement a protocol to ensure that immediate steps are taken after a breach to ensure that no further unauthorized access is permitted.

It was noted that patient information system in use in the hospital was similar to those used throughout the province, designed to provide broad access rather than to restrict access. These systems may permit access according to "role-based" access privileges (for example the role of a nurse is given broad access) or "location-based" access privileges where the system is shared across multiple locations or sites. It was noted that the rationale for not incorporating stricter access controls in a hospital setting is that if the patient information is not readily accessible in an emergency, the patient's health or safety would be at risk. The Commissioner was satisfied that the VIP flag system employed by the hospital met accepted standards.

Further information can be found at http://www.ipc.on.ca/images/Findings/up-HO_002.pdf

Example 6

Another case in Ontario involved a diagnostic imaging technologist who viewed (used) a woman's personal health information through the hospital's electronic health record. This was the same hospital referenced in the above example. The technologist, who had not provided health care to the patient, was the former spouse of the complainant's current spouse.

The patient requested a list of all individuals who accessed her record over a two-year period. The hospital conducted an investigation and determined that the technologist had viewed the patient's personal health information on 6 separate occasions, in contravention of Ontario's *Personal Health Information Protection Act*. The technologist was suspended without pay for three days and was required to undergo counseling and privacy re-training. The patient was not provided with information about the whether the technologist had been disciplined as a result of the breach.

The patient complained about the breach to Ontario's Information and Privacy Commissioner. The Commissioner commented that technical safeguards in place at the time of the previous case may have been appropriate then, but it may now be possible to limit employee's access to only those patients to whom they are providing health care. The Commissioner recommended that the hospital investigate whether there are technical solutions available to better protect the privacy of patient information. The Commissioner ordered the hospital to add to its breach investigation process a requirement that an agent or employee, who had contravened the Act, sign a confidentiality undertaking and non-disclosure agreement.

Additional information can be found at http://www.ipc.on.ca/images/Findings/ho-010.pdf

Manitoba Ombudsman

RESPONSE TO THE RECOMMENDATIONS UNDER

THE PERSONAL HEALTH INFORMATION ACT

CASES 2011-0513 AND 2011-0514

CANCERCARE MANITOBA

PRIVACY COMPLAINTS: USE OF PERSONAL HEALTH INFORMATION AND SECURITY OF PERSONAL HEALTH INFORMATION

SUMMARY: On August 3, 2012, CancerCare Manitoba provided its response to the Ombudsman, accepting all of the recommendations. CancerCare requested additional time to comply with some of the recommendations and the Ombudsman agreed that the proposed time frames for implementation were reasonable.

RESPONSE TO THE RECOMMENDATIONS

Under subsection 48(4) of *The Personal Health Information Act*, CancerCare Manitoba was required to respond in writing to the Ombudsman within 14 days of receiving the Ombudsman's report dated July 20, 2012. On August 3, 2012, CancerCare responded to the Ombudsman, accepting all of the recommendations.

Under PHIA, a trustee has 15 days from the date of acceptance to comply with the recommendations. CancerCare requested that we allow additional time for implementing some of the recommendations and we agreed that the proposed time frames were reasonable. Going forward, the actions taken by CancerCare to implement the recommendations will be monitored.

Below are the details of CancerCare's response to each of the recommendations, which have been provided to the complainant:

1. The Ombudsman recommends that CancerCare Manitoba send a letter to the complainant, apologizing for the employee's breach of privacy.

   Accepted.

   CancerCare Manitoba will send a letter to the complainant in accordance with subsection 48(6) of the Act. It will be forwarded to the complainant with a copy to your office no later than August 18, 2012.

2. The Ombudsman recommends, in accordance with section 6 of the Regulation, that CancerCare Manitoba conduct ongoing PHIA training for all staff and that such training be tracked by CancerCare.

   Accepted.

   CancerCare Manitoba will continue to conduct ongoing PHIA training for all staff.

   Regarding implementation of a PHIA training tracking mechanism, work on this has already begun. As we intend to leverage our in-house payroll application to do so, the reporting functionality requires testing and adoption of an intradepartmental process is necessary. Therefore we respectfully request an extension to August 31, 2012.

3. The Ombudsman recommends, in accordance with subsection 8(1) of the Regulation, that CancerCare conduct an audit of its security safeguards every two years, including administrative, technical and physical safeguards.

   Accepted.

   Efforts to support successful Privacy Compliance Audit (as was conducted in March, 2011), comprising administrative and physical safeguards will continue and the audit has been adopted as "best practice" within the organization. CancerCare Manitoba will continue to identify opportunities to improve this audit to incorporate technical safeguards as recommended. Work on this will continue within the Fall 2012 and be completed in the winter of 2013.

4. The Ombudsman recommends that CancerCare investigate which modules within its ARIA system offer an audit trail when personal health information is printed and provide the findings to our office.

   Accepted.

   CancerCare Manitoba Information Services Department has confirmed that an audit trail currently exists when the following reports are printed in ARIA:

   Audit Printed documents preview reports by user
   Physician Prescription Report
   Physician Prescription Report with dispensing information

   CancerCare Manitoba Information Services Department has engaged our Vendor, Varian, to determine when other future ARIA version upgrades will allow for an audit trail. We are requesting an extension to September 28, 2012 to allow sufficient time for review and input from the Vendor.

5. The Ombudsman recommends that CancerCare ensure its security practices adhere to the Guideline for Auditing Records of User Activity.

   Accepted.

   CancerCare Manitoba will strengthen and expand its auditing process in adherence to the Minister's Guidelines Guideline for Auditing of User Activity. Auditing of user activity will begin in the Fall 2012, coordinated by the PHIA Privacy Officer working closely with respective Managers within our organization.

6. The Ombudsman recommends that CancerCare, further to developing a formalized plan for auditing its electronic personal health information, provide our office with a report on its plan on how it will detect unauthorized use and disclosure of personal information.

   Accepted.

   CancerCare Manitoba is committed to this project. As the plan will involve consultation with many stakeholders internally and externally to develop a new role-based security model that will control accessibility, define patient chart access based on specific location of care delivery, and provide enhanced auditing reports, we are anticipating providing a formalized project plan in Fall 2012. Project completion is on track for June 2013.

7. The Ombudsman recommends that, when investigating and responding to any future privacy breach of this kind, CancerCare proactively communicate with the affected individual to ensure the individual knows the specific personal health information that was breached, when and why it was breached, and the steps that CancerCare has taken and will be taking to protect the individual's privacy in the wake of the breach.

   Accepted.

   For any future substantiated breaches of this kind, a meeting with the affected individual will occur to discuss the breach events and ensuring the individual's questions are answered. CancerCare Manitoba will advise the individual of his or her right to request a copy of the patient access log. If requested, CancerCare Manitoba staff will review the patient access log in his/her presence and inform the individual of his or her rights under the Personal Health Information Act accordingly. This process will be implemented immediately.

Mel Holley
Acting Manitoba Ombudsman