Manitoba Ombudsman

REPORT WITH RECOMMENDATIONS ISSUED ON JUNE 9, 2011

AND

RESPONSE TO THE RECOMMENDATIONS

UNDER

THE PERSONAL HEALTH INFORMATION ACT

CASE 2011-0079

FLIN FLON CLINIC

PRIVACY COMPLAINT INITIATED BY OMBUDSMAN: FAILURE TO DESTROY PERSONAL HEALTH INFORMATION IN A SECURE MANNER

PROVISIONS CONSIDERED: 17(1), 17(2), 17(3), 25(3) and REGULATION 245/97

PUBLICLY RELEASED ON NOVEMBER 28, 2011

SUMMARY OF REPORT WITH RECOMMENDATIONS AND RESPONSE

The Ombudsman initiated a complaint pursuant to subsection 39(4) of *The Personal Health Information Act* (the Act) following the report of a privacy breach. The Ombudsman investigated and found that the Flin Flon Clinic (the trustee) was not in substantial compliance with the requirements of the Act or the Personal Health Information Regulation (the Regulation) regarding destruction of information. Accordingly, the Ombudsman recommended actions to bring the trustee into compliance with the Act and Regulation.

The trustee accepted the recommendations made by the Ombudsman and demonstrated that it had complied with the recommendations, although not within the timeframes specified in the Act.

Manitoba Ombudsman

REPORT WITH RECOMMENDATIONS UNDER

THE PERSONAL HEALTH INFORMATION ACT

CASE 2011-0079

FLIN FLON CLINIC

PRIVACY COMPLAINT INITIATED BY OMBUDSMAN: FAILURE TO DESTROY PERSONAL HEALTH INFORMATION IN A SECURE MANNER

PROVISIONS CONSIDERED: 17(1), 17(2), 17(3), 25(3) and REGULATION 245/97

REPORT ISSUED ON JUNE 9, 2011

SUMMARY: The Ombudsman initiated a complaint pursuant to subsection 39(4) of *The Personal Health Information Act* (PHIA or the Act) following the report of a privacy breach. The Ombudsman investigated and found that the Flin Flon Clinic (the Clinic) was not in substantial compliance with the requirements of PHIA or the Personal Health Information Regulation (the Regulation). Accordingly, the Ombudsman recommended actions to bring the trustee into compliance with the Act and Regulation.

THE COMPLAINT

Our office was alerted by a third party to the fact that partially burned medical records containing personal health information (the records) were found blowing on and around a highway and gravel pit approximately 10 kilometers west of Flin Flon, Manitoba. A review of the records revealed that they were records from the Clinic.

The information received by our office raised issues with respect to the security of the personal health information maintained by the Clinic. In particular, the information received raised concerns about the Clinic's policy and practice with respect to the destruction of personal health information in a manner that protects the privacy of the individual(s) the information is about. Accordingly, a complaint was initiated by our office under Part 5, subsection 39(4) of PHIA which provides as follows:

> ***Ombudsman may initiate a complaint***
> ***39(4)*** *The Ombudsman may initiate a complaint respecting any matter about which the Ombudsman is satisfied there are reasonable grounds to investigate under this Act.*

Our investigation focused on the adequacy of the Clinic's policy and/or practice with respect to the requirement to destroy personal health information in a secure manner.

POSITION OF FLIN FLON CLINIC

During our investigation the Executive Director of the Clinic (the trustee) acknowledged that a privacy breach had occurred in the course of destroying medical records. In response to our inquiries, the trustee confirmed that arrangements were made to have an employee destroy a large volume of medical records relating to deceased patients for the period from 1976 to 1990. The trustee had understood that the employee would be destroying the records by burning them in an incinerator in a private and confidential manner. Upon learning of the breach, the trustee immediately instructed the employee to stop burning records.

The trustee advised that the 400 records and 6 boxes of papers scheduled for destruction were removed from the Clinic by the employee. The trustee further advised that all of the records and boxes removed from the Clinic had been destroyed. During our investigation, the trustee acknowledged that the incinerator the employee had used to burn the medical records was actually a "burn barrel". The trustee further acknowledged that some of the records may have escaped from the barrel during the burning process as the barrel did not have a cover.

Since the breach, the trustee has retrieved the partially burned records from the third party who had recovered them. The trustee has also instructed the employee to return to the site on several occasions to search for and retrieve any other partially burned medical records remaining there. The trustee advised our office that the employee found another 10 pieces of partially burned paper at the site, which have been returned to the Clinic. The trustee confirmed that the employee is not in possession of any more medical records.

The trustee noted that, in relation to the number of records actually destroyed by the employee, only a small number of partially burned records appear to have escaped from the barrel. The trustee determined that the risk associated with the breach in terms of harm/damage to reputation of individuals and identity theft/fraud was minimal based upon the location of the breach, the age of the records and the fact that all of the patients whose privacy was breached were deceased. The trustee also concluded that notification was not required in the circumstances.

The trustee advised that the Clinic had ceased operating on February 1, 2011. The trustee indicated that many of the Clinic's former patients have now had their records transferred to other health care facilities. The trustee further advised that any remaining medical records are currently being stored "under lock and key" in the basement of the Clinic building, pending transfer or eventual destruction.

The trustee provided our office with a copy of the *Flin Flon Clinic Policy Regarding Medical Files* (the Policy). Paragraphs 1 through 5 of the Policy provide that all medical files will be kept in a secure building for a minimum period of ten years from last patient encounter and that they will then be destroyed in a private and confidential manner. Paragraph 6 of the Policy states

that the trustee has contracted with a local business to destroy all medical information scheduled for destruction in a private and confidential manner by shredding same in a commercial shredder.

During our investigation, the trustee confirmed that paragraph 6 of the Policy was added after it became aware of the breach at issue. The trustee acknowledged that, prior to the breach, the Clinic did not have a written Policy regarding destruction and its practice had been to burn records scheduled for destruction at the local dump. The trustee had engaged the employee to destroy the records in an incinerator (burn barrel) on this occasion, as the dump had implemented a prohibition on burning.

ANALYSIS OF ISSUES AND FINDINGS

1. Do the records at issue contain *personal health information*?

The Act defines *personal health information* as:

> *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;*

The records found consisted of partially burned pages from what appeared to be medical clinic charts, as well as lab and other reports. The records included the names of patients of the Clinic, their dates of birth, addresses, diagnosis and treatments as well as the names of their doctors.

The Ombudsman found that the records at issue contain *personal health information*.

2. At the time of the breach, did the trustee have a written policy concerning the destruction of personal health information as required under the Act?

One of the stated purposes of PHIA is to establish rules governing the destruction of personal health information *in a manner that recognizes the right of individuals to privacy of their personal health information*.

In this regard, PHIA requires a trustee to establish a *written policy* concerning the destruction of personal health information and to ensure that personal health information is destroyed in a

manner that preserves the confidentiality of the information and protects the privacy of the individual(s) the information is about. Section 17 of the Act provides as follows:

> ***Retention and destruction policy***
> ***17(1)*** *A trustee shall establish a written policy concerning the retention and destruction of personal health information and shall comply with that policy.*
>
> ***Compliance with regulations***
> ***17(2)*** *A policy under subsection (1) must conform with any requirements of the regulations.*
>
> ***Method of destruction must protect privacy***
> ***17(3)*** *In accordance with any requirements of the regulations, a trustee shall ensure that personal health information is destroyed in a manner that protects the privacy of the individual the information is about.*

With respect to the destruction of personal health information, Regulation 2 of the *Personal Health Information Regulation* requires that:

> ***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, including measures*
> *(i) to ensure the security of the personal health information when a record of the information is removed from a secure designated area, and*
> *(ii) to ensure the security of personal health information in electronic form when the computer hardware or removable electronic storage media on which it has been recorded is being disposed of or used for another purpose;*

Our investigation has revealed that although the trustee had a written Policy regarding retention of medical records at the time of the breach, the policy did not provide for the secure destruction of personal health information as required by the Act and Regulations. After learning of the breach at issue, the trustee advised that it revised the Policy to include a paragraph regarding destruction of medical records. Paragraph 6 of the revised Policy provides that medical records scheduled for destruction will be sent to a local business where they will be shredded in a commercial shredder in a private and confidential manner.

The Ombudsman found that, at the time of the breach, the trustee did not have a written Policy regarding the destruction of personal health information as required under the Act and Regulation.

3. Are the trustee's arrangements for future records destruction compliant with PHIA?

The Act defines an *information manager* as *a person or body that processes, stores or destroys personal health information for a trustee.* When a trustee contracts with an outside organization to provide information management services, section 25 of the Act provides as follows:

> ***Agreement required***
> ***25(3)*** *A trustee who wishes to provide personal health information to an information manager under this section must enter into a written agreement with the information manager that provides for the protection of the personal health information against such risks as unauthorized access, use, disclosure, destruction or alteration, in accordance with the regulations.*
>
> ***Information manager must comply with Act***
> ***25(4)*** *An information manager shall comply with*
> *(a) the same requirements concerning the protection, retention and destruction of personal health information that the trustee is required to comply with under this Act; and*
> *(b) the duties imposed on the information manager under the agreement entered into under subsection (3).*
>
> ***Information deemed to be maintained by the trustee***
> ***25(5)*** *Personal health information that has been provided to an information manager under an agreement described in subsection (3) is deemed to be maintained by the trustee for the purposes of this Act.*

The trustee's revised Policy regarding the destruction of personal health information provides that it has contracted with a local business, an outside organization, *to destroy any and all medical information that is subject for destruction*. During the course of our investigation, the trustee advised that it did not have a written agreement with the local business, an information manager, regarding the destruction of personal health information as required under the Act.

The Ombudsman found that the Clinic's arrangements for the destruction of personal health information are not in compliance with the Act as an Information Manager Agreement is required.

SUMMARY OF FINDINGS

1. The Ombudsman found that the records at issue contain *personal health information*.

2. The Ombudsman found that, at the time of the breach, the trustee did not have a written Policy regarding the destruction of personal health information as required under the Act and Regulation.

3. The Ombudsman found that the trustee's arrangements for the destruction of personal health information are not in compliance with the Act as an Information Manager Agreement is required.

RECOMMENDATIONS:

Based on the above findings, the Ombudsman is recommending that the trustee:

1. Enter into a formal Information Manager Agreement, pursuant to subsection 25(3) of the Act, with the with the local business that it has contracted with to destroy any and all medical information that is subject to destruction under its Policy.

2. Consult with Manitoba Health for assistance in implementing the foregoing recommendation and familiarize itself with the resources available to trustees on Manitoba Health's website, in particular, *A Trustee's Guide to: Information Manager Agreements Required by The Personal Health Information Act* and *A Brief Summary for Information Managers*.

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 fax to the trustee on this date, the trustee shall respond by June 23, 2011. 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 did 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 on the Internet. Publication of this report on the Ombudsman's website will occur when this case has been concluded.

June 9, 2011
Irene A. Hamilton
Manitoba Ombudsman

Manitoba Ombudsman

RESPONSE TO THE RECOMMENDATIONS UNDER

THE PERSONAL HEALTH INFOMRATION ACT

CASE 2011-0079

FLIN FLON CLINIC

PRIVACY COMPLAINT INITIATED BY OMBUDSMAN: FAILURE TO DESTROY PERSONAL HEALTH INFORMATION IN A SECURE MANNER

PROVISIONS CONSIDERED: 17(1), 17(2), 17(3), 25(3) and REGULATION 245/97

SUMMARY: On June 16, 2011 the trustee provided the Ombudsman with a "draft" copy of an Information Management Agreement by facsimile, demonstrating that it was in the process of complying with the recommendations. On August 30, 2011 the trustee provided its formal response to the Ombudsman, accepting the recommendation to enter into an Information Management Agreement. The trustee subsequently demonstrated that it had complied with both recommendations.

RESPONSE TO THE RECOMMENDATIONS

Under subsection 48(4) of *The Personal Health Information Act* (the Act), the Flin Flon Clinic (the trustee) was required to respond to the Ombudsman's report in writing within 14 days of receiving the report. As the report was sent by facsimile on June 9, 2011 the trustee had until June 23, 2011 to respond. The trustee's response was to 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.*

The trustee did not provide a written response to the Ombudsman's recommendations by June 23, 2011 as required. However, the trustee did provide a "draft" copy of an Information Management Agreement to the Ombudsman by facsimile dated June 16, 2011, thereby demonstrating that it was in the process of complying with the recommendations.

The trustee did not provide a written response to the recommendations until August 30, 2011 when it advised as follows:

1. **The Ombudsman recommended that the trustee enter into a formal Information Management Agreement, pursuant to subsection 25(3) of the Act, with the local business that it has contracted with to destroy any and all medical information that is subject to destruction under its Policy.**

   The Flin Flon Clinic advised that it was accepting the Ombudsman's recommendation to enter into a formal Information Manager Agreement.

2. **The Ombudsman recommended that the trustee consult with Manitoba Health for assistance in implementing the foregoing recommendation and familiarize itself with the resources available to trustees on Manitoba Health's website, in particular, *A Trustee's Guide to: Information Manager Agreements Required by The Personal Health Information Act* and *A Brief Summary for Information Managers.***

   Although the Flin Flon Clinic did not specifically address this recommendation in its August 30, 2011 response, it subsequently confirmed that it had consulted with Manitoba Health in preparing the Information Manager Agreement.

Subsection 48(6) of the Act required the trustee to comply with the recommendations within 15 days of acceptance or within an additional period of time if the Ombudsman considered it to be reasonable. The trustee did not comply with the recommendations within 15 days of acceptance and did not advise the Ombudsman that it required an additional period of time to comply with the recommendations. The trustee did not demonstrate that it had complied with the Ombudsman's recommendations until November 2, 2011 when it provided a signed copy of an Information Management Agreement to the Ombudsman by facsimile.

Irene A. Hamilton
Manitoba Ombudsman