



Information and Privacy
Commissioner/Ontario

Commissaire à l'information
et à la protection de la vie privée/Ontario

Personal Health Information Protection Act

REPORT

FILE NO. HR10-18

Watson's Pharmacy and Wellness Centre



Tribunal Services Department
2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

Services de tribunal administratif
2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

Tel: 416-326-3333
1-800-387-0073
Fax/Télé: 416-325-9188
TTY: 416-325-7539
<http://www.ipc.on.ca>

Personal Health Information Protection Act

REPORT

FILE NO.

HR10-18

HEALTH INFORMATION CUSTODIAN: **Watson's Pharmacy and Wellness Centre**

SUMMARY OF INFORMATION GIVING RISE TO THE INVESTIGATION

On March 12, 2010, the owner of Watson's Pharmacy and Wellness Centre notified the Office of the Information and Privacy Commissioner/Ontario (IPC) that records containing personal health information were found scattered on Maloney Boulevard in Gatineau, Quebec. The owner advised that the records were prescriptions dating from 1994. The prescriptions related to thousands of patients of Nelson Drugs, the predecessor of the pharmacy which he now currently owns and operates as Watson's Pharmacy and Wellness Centre located on Main Street in Ottawa, Ontario. The IPC immediately began working with the owner in his role as health information custodian to ensure that the records were retrieved and secured. The IPC then commenced a review of this incident, pursuant to section 58 of the *Personal Health Information Protection Act, 2004* (the Act).

IPC PAST PRECEDENTS

Before discussing the details of this investigation, it is important to highlight the past precedents of the IPC with regards to similar incidents. Two previous incidents in which records of personal health information were found scattered on the street resulted in the IPC issuing Orders HO-001 in 2005 and HO-006 in 2009.

HO-001

In 2005, the IPC was made aware of records of personal health information blowing through the streets of downtown Toronto. Our investigation determined that the intersection of Wellington and York Streets had served as the location for a film shoot about the September 11, 2001 terrorist attack on New York's World Trade Center. The production company used the health records in the film shoot as special effects, believing that they were scrap paper. The records had been mistakenly sent by an X-ray and ultrasound clinic for recycling, rather than shredding, and had thus made their way onto the film set.

In Order HO-001, the IPC concluded that:

A health information custodian's responsibility to securely dispose of personal health information can only be met through the permanent destruction of those records, for example through irreversible shredding such as "cross-cut" shredding. The personal health information contained in these records must be obliterated to render them irreversible and to ensure that reconstruction of the information is virtually impossible.

In addition, Order HO-001 contained extensive order provisions directed to both the health information custodian and its agent, the paper disposal company, involved in the incident. In relation to this investigation and of particular relevance to this incident, the health information custodian was ordered to:

- review and amend its information practices to ensure that records of personal health information in its custody or control are securely stored and protected against theft, loss and unauthorized use or disclosure;
- put into place a written contractual agreement with any agent it retains to dispose of records of personal health information setting out the obligation for secure disposal and requiring the agent to provide written confirmation through an attestation once secure disposal has been conducted; and
- ensure that no unauthorized person will have access to the personal health information between the time the records leave the health information custodian's custody until their actual destruction.

HO-006

In December of 2008, the IPC was again contacted about an incident involving records of personal health information found scattered on the streets, this time outside a medical laboratory in Ottawa. Following a review, in 2009, Order HO-006 was issued which concluded that the health information custodian failed to comply with the *Act*, and ordered the custodian to take the following measures:

- implement its plan to place cross-cut shredders in every location and provide my office with documentation to serve as evidence of its completion; and
- ensure that all contracts or agreements in place with third party shredding companies comply with the requirements set out in HO-001, binding the shredding company to the requirements of the *Act* and its contractual agreement with the health information custodian. Specifically, all contracts or agreements must:
 - a. Set out the obligation for secure disposal, including how the records will be disposed of, under what conditions, and by whom. Secure disposal must consist

of permanently destroying paper records by irreversible shredding or pulverizing, thereby rendering them unreadable.

b. Require the shredding company to provide confirmation through a written attestation or certificate of destruction once the secure disposal has been conducted. This document must confirm the fact of the destruction, as well as, the date, time and location of destruction, and the name and signature of the operator who performed the secure destruction.

In addition to the above, in October 2009, as a result of this second incident, the IPC issued the best practice document, *“Get rid of it Securely to keep it Private: Best Practices for the Secure Destruction of Personal Health Information”* in partnership with the National Association for Information Destruction (NAID). The publication outlines a number of best practices that can be employed in the secure destruction of records of personal health information, including;

- developing a secure destruction policy that is clear, understandable and leaves no room for interpretation;
- segregating and securely storing records of personal health information;
- documenting the destruction process;
- developing criteria for selecting a third-party service provider;
- properly disposing of securely destroyed materials; and
- auditing and ensuring compliance with the secure destruction policy.

THE INVESTIGATION

Our office was advised that the health information custodian, who is the person that currently operates Watson’s Pharmacy and Wellness Centre, purchased the pharmacy in 2006. When he assumed possession of the pharmacy, there were a number of items left in the basement including signs from previous pharmacies, fixtures, and 6-10 black garbage bags and their contents. In March, 2010, the custodian began to make efforts to remove the garbage from the basement of the pharmacy. The custodian advised that he and his staff loaded the garbage into a rented garbage trailer but at no time did they check through the garbage bags to see what they contained as it appeared to be waste and debris from previous owners. The custodian further advised that there was nothing that would have indicated that records of personal health information were contained within the bags, particularly since patient records created by previous owners had been properly labeled and stored when he took possession of the pharmacy. Once the trailer was filled, the custodian contacted the contractor to secure the contents of the trailer and remove it from the premises.

Around 10 a.m. on March 12th, the custodian advised that he received a call from an individual who informed him that there were documents scattered on Maloney Boulevard in Gatineau, Quebec which belonged to the pharmacy. The health information custodian immediately called the Ontario College of Pharmacists and the IPC to seek advice in containing this breach. In

In addition, a representative of the custodian and the contractor who had been hired by the custodian to remove the garbage were immediately dispatched to Maloney Boulevard to contain the breach, including searching a one mile area to retrieve any materials that contained personal health information or other debris. The following day, March 13th, a second search was conducted and any remaining records were also retrieved. In total, the custodian advised that one garbage bag full of materials had been retrieved. At the direction of the IPC, the custodian has secured the records in an area of the pharmacy where other confidential patient information is kept.

Following this incident, the representative of the custodian and the contractor went to the Centre de Tri et de Revalorisation des Matériaux Secs de l'Outaouais to ensure the remaining garbage, including records of personal health information, had been duly processed. The supervisor confirmed for them that all discarded material had been processed and sent to the Waste Management Landfill in Cascades, Quebec. The custodian advised the IPC that the following process was followed:

- the contractor deposited the garbage into a large dump pile;
- a front-loader then loaded the garbage into a large automatic sorting facility;
- all paper product was separated and pulverized in preparation for the landfill (the supervisor and contractor confirmed that it would have been unreadable after this process); and finally,
- the paper product was separated into a large, covered dumpster and taken to the Cascades landfill where it was mixed with soil and added to the landfill.

As part of the investigation, the custodian provided the IPC with a copy of its Policy and Procedures Manual (the Manual) which includes a comprehensive section on privacy. In addition to outlining the roles and responsibilities of staff in protecting personal health information under the *Act*, the Manual also states that staff shall sign an acknowledgement indicating that they are aware of, and will comply with, the Manual. Staff must also sign an acknowledgement when they receive any additional privacy training as a result of policy or procedural changes as well as a confidentiality agreement as part of their standard employment contract.

In addition to the above, the custodian advised that it had implemented new procedures as a result of this incident. Specifically, the custodian has made the following practice changes:

- all garbage will be kept in clear bags which can easily be examined before disposal;
- any existing garbage that has not been packed by the current staff will be personally checked by the custodian and transferred into clear bags;
- personal health information will only be retained for a two-year period, as required by the College of Pharmacists of Ontario; and
- patient prescription bottles with old drugs will no longer be accepted at the pharmacy. Instead, if patients bring in old pill bottles with drugs to be disposed of, pharmacy staff will take the drugs and dispose of them, returning the bottle to the patient to discard themselves.

Staff of the custodian have been briefed on the new procedures and each staff member has signed an acknowledgement stating that they are aware of the procedural changes. Each staff member met with the representative of the custodian on a one-on-one basis to discuss the new procedures and any questions they might have. In addition to the staff briefing, existing procedures were also re-articulated with a focus towards the importance of safeguarding personal health information.

In order to fulfill their obligations under section 12(2) of the *Act* to notify patients at the first reasonable opportunity about this incident, the health information custodian posted a notice describing this incident on the pharmacy's website. In addition, the custodian posted signs in the pharmacy so that patients could be notified of this breach and have any questions answered. To date, the custodian advised that it had not received any calls from patients about this incident.

INVESTIGATION RESULTS

I am satisfied that M.S. Watson Health Care Inc., the operator of Watson's Pharmacy and Wellness Center, is a health information custodian pursuant to section 3(1)4iii of the *Act*. This section extends the definition of health information custodian to include the person who operates a pharmacy within the meaning of Part VI of the *Drugs and Pharmacies Regulation Act*.

Based on the facts of this incident, it is apparent that section 13(1) of the *Act*, in conjunction with section 1(5.1) of Regulation 329/04, was breached. These sections require a health information custodian to ensure that records of personal health information in its custody or control are retained, transferred and disposed of in a secure manner. Similarly, section 12(1) of the *Act* was also breached. This section requires a health information custodian to take reasonable steps to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that records of personal health information are protected against unauthorized copying, modification or disposal.

I want to acknowledge the quick action taken by the health information custodian in reacting to this incident. The custodian took immediate steps to contain the breach and to ensure that records were either retrieved or had been securely destroyed. Further, the custodian worked in full cooperation with our office to ensure that staff were made aware of their obligations under the *Act* and that measures were put in place to ensure that a similar incident would not happen again. Finally, steps have been taken to bring this breach to the attention of the pharmacy's patients. I applaud the custodian for these actions.

Based on the above, I am satisfied that the health information custodian has taken all the necessary steps to address this breach. In these circumstances, no further action is required and it is not necessary for me to make any order provisions.

The person who currently operates the pharmacy is the health information custodian and must bear responsibility for the failure to securely dispose of the records of personal health information. However, based on the information provided by the custodian, it would appear that the previous operators of the pharmacy failed to either securely transfer or dispose of records of

personal health information in an appropriate manner – had they done so, this incident may not have occurred. I will address this issue in the next section.

THE LIFECYCLE OF RECORDS OF PERSONAL HEALTH INFORMATION

It is regrettable that the IPC is once again investigating a situation in which records of personal health information were found on the streets. Four years ago, we issued our first order under the *Act*, Order HO-001, which involved records of personal health information that were found scattered across the streets of downtown Toronto. Again last year, we issued an order, Order HO-006, involving health records that were found on the street outside a medical centre in Ottawa.

In this case, the records of personal health information that were found scattered in Gatineau, Quebec, had been in the possession of at least four different operators of the pharmacy over the course of more than fifteen years. Based on the information gathered by our investigation, the personal health information of countless patients was left vulnerable to theft, loss and unauthorized use or disclosure for this period of time. While the *Act* did not come into effect until 2004, safeguards should have been put in place by all four operators of the pharmacy who had custody and control of the records.

Had the pharmacist who created the records initially ensured that adequate safeguards were in place before selling the practice to the next practitioner, this incident might not have occurred. The records would have either been stored in a secure fashion or, if they did not need to be retained, securely destroyed. Subsequently, at each step along the way, as new operators assumed control of the pharmacy, the personal health information records were not properly protected from theft, loss or unauthorized use or disclosure.

It is critical for health information custodians to be aware that the *Act* imposes duties on all custodians who have custody or control of health records, even if that custody or control is subsequently passed on to another custodian.

This incident highlights a number of important lessons for all health information custodians.

The *Act* requires health information custodians to ensure that records of personal health information are retained, transferred and disposed of in a secure manner. It also requires custodians to take steps that are reasonable in the circumstances to ensure that personal health information is protected against theft, loss and unauthorized use or disclosure and that health records are protected against unauthorized copying, modification or disposal.

Under the *Act*, health information custodians remain responsible for records of personal health information until complete custody and control of these records is transferred to a person who is legally authorized to assume their custody and control. This means that, when a health practice is being sold, the health information custodian selling the practice remains responsible for the secure retention, transfer and disposal of these records until complete custody and control is transferred to a purchaser who has the legal authority to assume custody and control.

Health information custodians must ensure that records of personal health information that are required to be retained are being retained in a secure manner. This includes records that are required to be retained in accordance with the retention period in applicable legislation, standards of practice and standards of professional conduct. The *Act* also requires health information custodians with custody or control of personal health information that is the subject of a request for access to retain the personal health information for as long as necessary to allow the requester to exhaust any recourse that the individual may have with respect to the request for access under the *Act*.

In retaining records of personal health information in a secure manner, health information custodians must implement physical, administrative and technical safeguards commensurate with the amount and sensitivity of the personal health information retained. Consideration must be given to the number and nature of employees and agents with access to the personal health information and with the threats and risks associated with the personal health information. This includes retaining paper records in locked cabinets and restricting access to locations within the premises where these records are retained. For additional information and best practices relating to the secure retention of records of personal health information, please refer to *Fact Sheet 1: Safeguarding Personal Health Information* published by the Information and Privacy Commissioner of Ontario, available at www.ipc.on.ca.

The *Act* imposes conditions that must be satisfied prior to disclosing or transferring personal health information to a potential successor. Health information custodians may disclose personal health information to a potential successor to allow them to assess and evaluate the operations, provided that the potential successor first enters into a confidentiality agreement. This agreement must clearly state that the potential successor agrees to keep the personal health information confidential and secure and agrees not to retain the personal health information for longer than is necessary for the purpose of the assessment or evaluation.

In addition, health information custodians may only transfer records of personal health information to a successor if the health information custodian makes reasonable efforts to give notice to the individuals to whom the records relate before transferring the records or, if that is not reasonably possible, as soon as possible thereafter.

Health information custodians must also ensure that records of personal health information in their custody or under their control are transferred to a successor in a secure manner. This requires an agreement between health information custodians and their successors in relation to the records being transferred. In this regard, the agreement should describe the records of personal health information that are being transferred, including the nature and type and date of the records being transferred and the location within the premises where the records are being securely retained. It is simply not sufficient for health information custodians to leave records of personal health information on the premises without advising the successor which records are being transferred and where these records are being securely retained.

Records of personal health information that are not required to be retained must be disposed of in a secure manner such that reconstruction is not reasonably foreseeable in the circumstances. In selecting the precise method for securely disposing of records of personal health information in

paper and electronic format, attention must be given to the *Act* and its regulation; with orders issued by this Office, including Order HO-001 and Order HO-006; and with IPC guidelines, fact sheets and best practices, including *Fact Sheet 10: Secure Destruction of Personal Information*. These are all available on the IPC website at www.ipc.on.ca.

The secure retention of records of personal health information pending their secure disposal must also be ensured. At a minimum, the records intended for secure disposal should be physically segregated from other records and from refuse, a secure area should be designated for the retention of the records prior to their disposal and the records should be retained in a clearly marked and locked container.

In the event that records of personal health information will be securely disposed of by a third party service provider, custodians must also ensure that the records are transferred to the third party service provider in a secure manner.

An agreement must also be entered into with the third party service provider that sets out their responsibilities in securely disposing of the records of personal health information, that identifies the time frame within which the records must be securely disposed of as well as the manner in which, and the conditions pursuant to which, the records must be securely disposed of. The agreement must also require the third party service provider to provide a certificate of destruction identifying the records of personal health information securely disposed of, setting out the exact date and time that the records were disposed of, identifying the method of secure disposal employed and bearing the name and signature of the individual(s) who performed the secure disposal. For sample contractual clauses, please refer to *Fact Sheet 10: Secure Destruction of Personal Information* published by the IPC.

In summary, this case highlights a number of important lessons for health information custodians, particularly in situations similar to this, where records of personal health information have passed through the custody and control of a succession of custodians. Health information custodians have duties and responsibilities imposed by the *Act* throughout the lifecycle of a record of personal health information. Those duties and responsibilities do not cease simply because records may be passed on to another custodian through the sale of a business. Similarly, custodians who are taking over an established business cannot assume that their predecessor has fully complied with the requirements of the *Act*. It is imperative that custodians who become new business owners ensure that records of personal health information coming into their possession are catalogued accurately and then either securely stored or securely disposed of in accordance with relevant legislation, standards of practice and standards of professional conduct.

May 21, 2010

Brian Beamish
Assistant Commissioner, Access