Information and Privacy Commissioner of Ontario

ORDER HO-006

Ann Cavoukian, Ph.D.
Commissioner
July 3, 2009

BACKGROUND:

On December 31, 2008, a member of the media notified the Office of the Information and Privacy Commissioner/Ontario (IPC) that records containing personal health information were found scattered on the street outside a medical centre housing a medical laboratory, located at 267 O'Connor Street in Ottawa, Ontario. The medical laboratory is owned and operated by CML HealthCare Inc. (CML). The IPC acted immediately to ensure that the records were secured that day and then commenced a review of this incident, pursuant to section 58 of the *Personal Health Information Protection Act, 2004* (the *Act*).

CML is a diagnostic services business that provides laboratory testing and medical imaging services. In its laboratory testing business, CML operates 125 licensed specimen collection centres across Canada and one licensed medical diagnostic laboratory. In their medical imaging business, CML provides services in five provinces across Canada, including: 83 in Ontario, one in Quebec, two in Manitoba, nine in Alberta, and 20 in British Columbia. Through their United States (U.S.) acquisition, American Radiology Services (ARS), CML also operates 17 outpatient medical imaging centres in Maryland and Delaware. In addition, ARS coordinates the provision of reading services with 11 Maryland hospitals and coordinates the provision of teleradiology service with 29 hospitals across six states in the U.S. to provide primary or secondary reading service via its teleradiology network.

Upon learning of the incident, I immediately contacted CML and spoke to the Imaging Manager at the laboratory in question. The Imaging Manager advised me that they were aware of the situation and had notified CML's Chief Executive Officer. They were in the process of conducting a thorough investigation.

According to the Imaging Manager, a parking attendant who was working in an adjacent lot noticed that records had fallen out of a recycling truck as it was leaving the premises. The attendant became concerned when he inspected the records and noticed that they contained personal health information such as names, Ontario health numbers and results of laboratory tests. The attendant picked up all the records that he was able to locate in and around the surrounding building and parking lot. The Imaging Manager advised that a further search of the area had been undertaken by laboratory staff and they believed that they were able to locate all the records that had been scattered.

IPC PRECEDENT – ORDER HO-001:

Before further discussing the details of this incident and the resulting review, it is critical to refer to Order HO-001, my first order under this *Act*, issued in October 2005. The incident resulting in that order was similar in nature as it involved records of personal health information that were found scattered on the street. In the 2005 incident, the records were blowing through the streets of downtown Toronto. As it turned out, 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 health 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. My office immediately initiated a review into the matter to determine how this had transpired.

Following the review, I issued Order HO-001, which dealt with the obligation imposed by the *Act* on a health information custodian to ensure that records of personal health information in its custody or under its control are disposed of in a secure manner. The Order emphasizes that recycling paper is not a substitute for secure destruction. In particular, I 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.

As a result, 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. The following order provisions are of particular relevance to this investigation. In Order HO-001, 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.

CONDUCT OF THE REVIEW:

Following my telephone conversations with the Imaging Manager on December 31, 2008, over the course of several hours, she assured me that all the records had been retrieved, and an IPC Investigator was then assigned to the file. On January 6, 2009, the Investigator visited the medical laboratory in Ottawa to further investigate the incident. The Investigator met with the Operations Manager for the Eastern Territory (Operations Manager) to tour the site and review the practices and procedures of the laboratory. During the site visit, the Investigator was advised by the Operations Manager that she concluded that the records of personal health information, which had ended up on the street on December 31, 2008, had mistakenly been

placed in a box designated for recycling rather than the box designated for shredding. Upon her review of the physical layout of the laboratory, the Operations Manager discovered that the blue recycling bin was located immediately beside the brown box, designated for off-site shredding. The Operations Manager advised the Investigator that she immediately moved the blue recycling bin to another room in order to ensure that personal health information could not be inadvertently placed into the recycling bin in future.

The Operations Manager further advised the Investigator that after being notified of this incident, she immediately sent a memorandum to all staff reminding them of the proper procedure for shredding records. The Operations Manager explained that the standard procedure at this location was to shred all records containing personal health information on-site. However, if the shredder was not working properly, the records are to be placed in a brown box designated for off-site shredding. These records are sent via CML's own courier to their corporate office, also located in Ottawa, for shredding by a commercial shredding company. The Operations Manager advised that this is a standard practice, as not all laboratories have shredders on site. Once the records are shredded, the Operations Manager indicated that CML receives a certificate of destruction from the shredding company.

The Operations Manager advised that following this incident, she immediately reviewed CML's policies with staff at the laboratory to ensure that they were aware of, and adhering to, the privacy and shredding policies. She stated that this provided a good opportunity to discuss the incident, as well as review a variety of privacy-related issues that might arise in a laboratory setting. The Operations Manager indicated that she intends to have in-house privacy training as a standing agenda item at each monthly team meeting so that issues can be raised and discussed regularly.

During the site visit, the Investigator was provided with copies of the following documents:

- Eight laboratory reports for eight different patients (retrieved by the parking lot attendant after they fell out of the recycling company's truck);
- Five receipts for two patients who paid for testing services at the lab (retrieved by the parking lot attendant after they fell out of the recycling company's truck);
- A copy of a January 5, 2009 memorandum to all staff from the Operations Manager regarding the proper shredding procedure to follow; and
- A sample copy of a Service Ticket that is provided by the commercial shredding company contracted by CML when the company picks up records for shredding. The Service Ticket states, "…the materials received on the above date will be confidentially handled and destroyed and the shredded material will then be recycled. A certificate of destruction will be included on your invoice."

While visiting the site, the Investigator also spoke with the parking lot attendant regarding his efforts to retrieve the records that had fallen out of the recycling truck. He advised that on the day of the incident, he was working in his booth when he noticed the truck from the recycling company arrive to pick up the recycling. Following the truck's departure, he noticed some sheets

of paper scattered around the parking lot and across the street. Upon further inspection, he realized that the papers contained personal health information of individuals who had visited the laboratory adjacent to the parking lot, including the names of these individuals and their physicians, health card numbers and clinical test results. The attendant then walked around the parking lot and surrounding area and picked up any additional papers that he could find. He advised that as he was picking them up, a member of the media, who had been informed about the incident by a passerby, arrived on the scene and he told the media what had happened.

Subsequently, the IPC was also provided with the following excerpts from CML's Privacy Code Manual:

- Tab 17: Principle 7: Safeguards
- Tab 18: Destruction of Personal Information Policy
- Tab 19: Physical and Security Safeguards

In addition, at my request, executives from CML, including the President, Chief Executive Officer; Executive Vice President, Chief Operating Officer; Executive Vice President, Corporate Development; and a Privacy Consultant to CML, attended at the IPC office to further discuss the incident and CML's response to it.

ISSUES ARISING FROM THE REVIEW:

I identified the following issues, which will be discussed in turn, as arising from this review:

(A) Are the records at issue "records" of "personal health information" as defined in sections 2 and 4 of the *Act*?

(B) Is CML a "health information custodian" as defined in section 3(1) of the *Act*?

(C) Did CML comply with section 13(1) of the Act and section 1(5.1) of Regulation 329/04 to the *Act*?

(D) Did CML comply with section 10(1) of the *Act*?

(E) Did CML comply with section 12(1) and (2) of the *Act*?

RESULTS OF THE INVESTIGATION:

Issue A: Are the records at issue "records" of "personal health information" as defined in sections 2 and 4 of the *Act*?

Section 2 of the *Act* defines a record as:

> a record of information in any form or in any medium, whether in written, printed, photographic or electronic form or otherwise, but does not include a computer program or other mechanism that can produce a record.

Section 4(1) of the *Act* states:

> In this Act,
>
> "personal health information", subject to subsections (3) and (4), means identifying information about an individual in oral or recorded form, if the information,
>
> (a) relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family,
>
> (b) relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual,
>
> (c) is a plan of service within the meaning of the *Long Term Care Act, 1994* for the individual,
>
> (d) relates to payments or eligibility for health care, or eligibility for coverage for health care, in respect of the individual,
>
> (e) relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance,
>
> (f) is the individual's health number, or
>
> (g) identifies an individual's substitute decision-maker.

Section 4(2) of the *Act* provides:

> In this section,
>
> "identifying information" means information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual.

Section 4(3) of the *Act* provides:

> Personal health information about an individual includes identifying information about the individual that is not personal health information described in subsection (1) but that is contained in a record that contains personal health information described in that subsection about the individual.

The records at issue are comprised of laboratory reports and receipts. The eight laboratory reports contain information relating to the individuals to whom laboratory testing services were provided including their name, date of birth, gender, Ontario health number and contact number, as well as information relating to the name and address of the requesting physician, the type of laboratory test ordered, the date of the test and the results. The five receipts that were retrieved also contain information relating to two individuals to whom services were provided including their name, gender and contact number, as well as information relating to the name and address of the requesting physician, the service provided and the amount of the fee paid to the laboratory.

Based on the above, I find that the records at issue are "records" of "personal health information" as defined in sections 2 and 4 of the *Act* as the records relate to the physical health and the provision of health care to the individuals, identify their providers of health care, relate to payments for health care and contain the health numbers of the individuals. CML does not dispute this finding.

Issue B: Is CML a "health information custodian" as defined in section 3(1) of the *Act*?

Section 3(1) of the *Act* states, in part:

> "health information custodian", subject to subsections (3) to (11), means a person or organization described in one of the following paragraphs who has custody or control of personal health information as a result of or in connection with performing the person's or organization's powers or duties or the work described in the paragraph, if any:
>
> [...]
>
> 4. A person who operates one of the following facilities, programs or services:
>
> […]
>
> iv. A laboratory or a specimen collection centre as defined in section 5 of the *Laboratory and Specimen Collection Centre Licensing Act*.

Section 5 of the *Laboratory and Specimen Collection Centre Licensing Act* defines a laboratory and a specimen collection centre, respectively, as follows:

> "laboratory" means an institution, building or place in which operations and procedures for the microbiological, serological, chemical, hematological, biophysical,

immunohematological, cytological, pathological, cytogenetic, molecular genetic or genetic examination, or such other examinations as are prescribed by the regulations, of specimens taken from the human body are performed to obtain information for diagnosis, prophylaxis or treatment;

[…]

"specimen collection centre" means a place where specimens are taken or collected from the human body for examination to obtain information for diagnosis, prophylaxis or treatment, but does not include,

(a) a place where a legally qualified medical practitioner is engaged in the practice of medicine or surgery,

(b) a place where a registered nurse who holds an extended certificate of registration under the *Nursing Act, 1991* is engaged in the practice of nursing, or

(c) a laboratory that is established, operated or maintained under a licence under this Act.

As previously mentioned, CML is a diagnostic services business that provides laboratory testing and medical imaging services. In their Canadian operations, CML conducts tests used by physicians to assist in the diagnosis of disease and patient treatment. These include: hematology, biochemistry, cytology, microbiology, histology, holter monitoring, prostate specific antigen and HPV testing. In its medical imaging business, CML provides medical imaging services including MRI, CT, nuclear medicine, ultrasound, mammography, x-ray, flouroscopy and bone densitrometry.

Based on the above, I find that CML is a "health information custodian" as defined in section 3(1)4(iv) of the *Act*. CML does not dispute this finding.

Issue C: Did CML comply with section 13(1) of the *Act* and section 1(5.1) of Regulation 329/04 to the *Act*?

Section 13(1) of the *Act* provides as follows:

A health information custodian shall ensure that the records of personal health information that it has in its custody or under its control are retained, transferred and disposed of in a secure manner and in accordance with the prescribed requirements, if any.

Section 1(5.1) of Regulation 329/04 to the *Act* provides:

In subsection 13(1) of the *Act,*

"disposed of in a secure manner" does not include, in relation to the disposition of records of personal health information, the destruction of the records unless the

> records are destroyed in such a manner that the reconstruction of the records is not reasonably foreseeable in the circumstances.

Based on the facts of this incident, it is evident that CML did not comply with its obligations under section 13(1) of the *Act*. Records containing personal health information were found on the streets of Ottawa and were accessed by at least one unauthorized individual, the parking lot attendant. Only his quick action contained what might have been a far more serious incident. These records were clearly not retained by CML in a secure manner. Similarly, they were not transferred or disposed of securely.

Our investigation found that the physical layout of the laboratory played a key role in the health information ending up on the streets. By having the blue recycling bin located directly beside the brown box designated for off-site shredding, the potential for human error was greatly increased. It appears that a staff member had inadvertently placed the records in the recycling bin. This unfortunate error led to the records intended for shredding being treated as if they were to be recycled and subsequently, falling out of the back of the recycling company's truck and being scattered onto the streets.

Based on all the above, I find that CML did not ensure that the records of personal health information in its custody or under its control were retained, transferred and disposed of in a secure manner. As a result, CML did not comply with section 13(1) of the *Act* and section 1(5.1) of Regulation 329/04 to the *Act*.

Issue D: Did CML comply with section 10(1) of the *Act*?

Section 10(1) of the *Act* provides as follows:

> A health information custodian that has custody or control of personal health information shall have in place information practices that comply with the requirements of this *Act* and its regulations.

During the course of this review, CML provided my office with a copy of its *Destruction of Personal Information Policy* (the Policy). This Policy is Tab 18 of CML's sixty-one page Privacy Code Manual.

Given the large volume of records of personal health information that each CML laboratory location handles on a routine basis, it is critical that their Policy for the secure disposal of those records be clear, understandable and leave no room for interpretation.

Our review of the Policy determined that a number of deficiencies existed. In general, I found it unclear and somewhat confusing - it left me doubtful that such incidents would not occur in the future.

For example, it provided that all sites were only to have cross-cut shredding machines "if physically possible." I agree that the cross-cut shredding of records of personal health information is an appropriate method of secure disposal. However, at the time of reviewing the Policy, CML did

not provide me with any information to indicate that the physical layout of any of its locations would not make it "physically possible" to have a cross-cut shredding machine on site.

While I understand that there may be some locations where space is limited, I could not accept, without concrete evidence, that it was not possible to house a shredding machine at all locations. We discussed this concern with CML, and to their credit, the Policy was amended to no longer include the qualifier, "if physically possible." Instead, it now simply states that, "Only cross-cut shredding machines are to be used." I am pleased that this important change has been made. CML has advised my office that they have begun a pilot project at fifteen CML locations. Each of those fifteen locations is now testing cross-cut shredders on-site, with the plan being to implement them across all sites in the coming months.

In addition, with respect to the particular incident that gave rise to this review, as stated earlier, the location of the bin designated for off-site shredding no doubt directly contributed to the health records ending up on the street. As noted earlier, this bin was positioned right next to the recycling bin, and a staff member had inadvertently placed the records in the wrong bin.

While the Policy required the shredding bin to be kept in a secure and locked area, there was nothing added to the Policy to prevent the shredding bin from once again being located next to the recycling container. To rectify this, CML added a specific direction in the Policy that shredding bins are to be kept in a separate location from all recycling bins. This will go a long way in limiting the risk of a staff member inadvertently discarding information intended for shredding, in the box designated for recycling.

The Policy also contained extensive provisions for those instances when shredding machines became inoperable. The "back-up plan" provided that, in the event that a shredding machine located at a laboratory became inoperable, then health records could be transferred to another CML site for destruction. In my view, the option of transferring records to another CML site would greatly increase the risk of theft, loss, and unauthorized use or disclosure; it did not strike me as an acceptable alternative. Nor was it clear how the records would be transferred to another site or by whom. These concerns were raised with CML and they amended their Policy to indicate that if a shredder becomes inoperable, all materials to be shredded will be kept in a secure, clearly marked container until a new cross-cut shredder is available. The Policy clearly states that materials to be shredded will not be transferred from one CML site to another. In the event that the volume of material to be shredded becomes excessive, the Policy now states:

> …the manager responsible for the facility should notify a CML contracted shredding company to shred the accumulated materials. A signed receipt for pick-up of the materials must be obtained, and a "certificate of destruction" must be provided by the designated shredding company following the shredding. Receipts and certificates must be retained at the site. The CML contracted shredding company shall sign a third party privacy protection contract.

I am very pleased with these changes and CML's revised plan to contact a contracted third party shredding company when a shredder becomes inoperable and shredding material becomes excessive.

I cannot emphasize enough, as we did with CML, the importance of having a written contract in place with any shredding company used to securely dispose of health records. This contract must set out the responsibilities of the shredding company in respect of secure disposal, including how the records will be disposed of, under what conditions and by whom, and require a written attestation or certificate of destruction. The certificate of destruction should confirm that the records were securely disposed of, including the date, time and location, and the name and signature of the person who securely disposed of them.

Having a written contract with a commercial shredding company, containing very clear and specific expectations with respect to secure disposal, and obtaining a written attestation or certificate of destruction is critical. This was stressed in Order HO-001:

> In order to ensure that a health information custodian's obligations under section 13(1) are met, the health information custodian, when engaging an agent to dispose of records, must enter into a written contractual agreement with that agent. The agreement should clearly spell out the responsibilities of the agent to securely destroy the personal health information records, how the destruction will be accomplished, under what conditions, and by whom. The agreement should also require the type of attestation of destruction….

Retaining a commercial shredding company to securely dispose of records of personal health information satisfies the requirements in section 13(1) of the *Act* and section 1(5.1) of the Regulation 329/04 to the *Act*. However, it must be done properly.

My office also reviewed other portions of CML's Privacy Code Manual. *Tab 17: Principle 7: Safeguards* pertains to the physical, organizational and technological methods implemented by CML to protect personal information, including personal health information, and addresses the importance of protecting the confidentiality of such information and meeting the requirements under section 12(1) and (2) and section 13(1) and (2) of the *Act*. My office found this section to be sufficient.

Similarly, my office reviewed *Tab 19: Physical and Security Safeguards* which outlines the physical and security measures to safeguard personal health. Again, there were no concerns with this section.

In addition, during this review, CML provided my office with its *Specimen Collection Centre Manual* (the Manual). All staff are provided with a copy of the Manual at the start of their employment. They are asked to review and sign the Manual to indicate that they have read and fully understood its contents. They are again asked annually to review and sign the Manual to acknowledge their understanding of its contents.

Section 16 of the Manual is entitled *Privacy, Personal Information Protection and Electronic Document Act and Personal Health Information Protection Act (Ontario)*. I note with respect to the federal PIPEDA, complaints are directed to the Privacy Commissioner of Canada. In discussions with CML, we noted that complaints relating to health information needed to be directed to my office since we had oversight over the *Personal Health Information Protection Act*. CML agreed and added this reference.

Given the above, I find that based on the information practices provided, and the changes that CML has made, CML has complied with section 10(1) of the *Act*.

Issue E: Did CML comply with section 12(1) and (2) of the *Act*?

Section 12(1) of the *Act* provides as follows:

> A health information custodian shall take steps that are reasonable in the circumstances 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 the records containing the information are protected against unauthorized copying, modification or disposal.

Section 12(2) of the *Act* provides as follows:

> Subject to subsection (3), and subject to the exceptions and additional requirements, if any, that are prescribed, a health information custodian that has custody or control of personal health information about an individual shall notify the individual at the first reasonable opportunity if the information is stolen, lost or accessed by unauthorized persons.

In light of my finding on non-compliance under Issue C, it is clear that CML did not take reasonable steps to ensure that personal health information in its custody or control was protected in accordance with section 12(1). Therefore, I find that CML did not comply with section 12(1).

Since I found that CML failed to take reasonable steps as required by section 12(1), I must now consider whether CML has complied with the notification requirement set out in section 12(2) of the *Act*.

A health information custodian that has custody or control of personal health information is required to notify the individual at the first reasonable opportunity if the personal health information is stolen, lost or accessed by unauthorized persons. It is not disputed that the personal health information at issue was accessed by at least one unauthorized person, that being the parking lot attendant.

In this regard, CML advised that all ten individuals, whose records of personal health information were involved in this incident, were contacted by telephone by the General Manager of Laboratory Services. Four were spoken to directly, and voicemail messages were left for the remaining six. When messages were not returned, CML sent a letter to each of these six individuals notifying them of the incident. One individual contacted the IPC directly to discuss the matter and was advised that we were already conducting an investigation.

In light of the above, I am satisfied that CML has complied with section 12(2) of the *Act* and met its obligation to notify the affected individuals.

SUMMARY OF FINDINGS:

I have made the following findings in this review:

1. The records at issue are "records" of "personal health information" as defined in sections 2 and 4 of the *Act*.

2. CML is a "health information custodian" as defined in section 3(1)4(iv) of the *Act*.

3. CML did not comply with section 13(1) of the *Act* and section 1(5.1) of Regulation 329/04 to the *Act* as it did not ensure that the records of personal health information in its custody or under its control were retained, transferred and disposed of in a secure manner.

4. CML has complied with section 10(1) of the *Act* as it now has information practices in place that comply with the requirements of the *Act* and its regulation.

5. While CML did not comply with section 12(1) of the *Act*, CML has complied with section 12(2) of the *Act*, fulfilling its obligation to notify individuals.

ORDER:

I order CML to:

1. Implement its plan to place cross-cut shredders in every location and provide my office with documentation to serve as evidence of its completion.

2. 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.

3. In order to verify compliance with this Order, I require that CML provide me with proof of compliance by September 25, 2009.

PARTNERSHIP WITH NAID TO DEVELOP AN INDUSTRY BEST PRACTICE

As indicated, Order HO-001 focused on the proper procedures that must be implemented to ensure the secure destruction of personal health information. In drafting HO-001, my office worked closely with the National Association for Information Destruction, or NAID:

> The National Association for Information Destruction, or NAID, is a national association that represents companies that specialize in secure information and document destruction. The mission statement of NAID Canada, the Canadian arm of NAID, is to raise awareness and understanding of the importance of secure information and document destruction. As such, NAID Canada offers programs and services based on a set of best practices for the proper management and destruction of sensitive documents. Their position on secure disposal of sensitive information is particularly relevant to health information custodians and their responsibilities for secure disposal under section 13(1) of the *Act*.

Given that personal health information is the "lifeblood" of its business and an indispensible part of the industry, CML has expressed a willingness to ensure that their staff understand that privacy is not only an obligation under the *Act,* but also an integral part of the standard of care. This includes ensuring that records of personal health information are retained, transferred and disposed of in a secure manner, in accordance with the *Act*.

In this regard, CML has advised that, as part of this year's Annual Managers' Meeting, managers from across Canada and the United States will be provided with an opportunity to attend a Workplace Privacy Workshop. CML has indicated that the topics will include the importance of protecting patient information, document handling, and employee privacy. Attendees will also be provided with the opportunity to discuss the privacy issues they face in each of their respective areas.

In its continued efforts to be a leader in this regard, and as a demonstration of its corporate responsibility, CML is going further. I am pleased to advise that CML has agreed to work in collaboration with my office and NAID to develop a practice direction for the secure disposal of records of personal health information. This document will serve as an industry "Best Practice" and will highlight the importance of ensuring that records of personal health information are securely disposed of by establishing standards and best practices for secure destruction.

COMMISSIONER'S MESSAGE:

It has been almost four years since my office issued its first order under the *Personal Health Information Protection Act*. That order dealt with a similar set of circumstances to those dealt with in this investigation – records of personal health information blowing freely in the streets of a major urban centre, due to the confusion between secure destruction and recycling.

When my office was contacted on December 31, 2008 regarding this incident, I was disheartened to say the least, to learn that after all these years and all the information sharing that has taken place, an incident so similar in nature to the one in our first order had occurred. It served as a reminder that while we may have come a long way in four years in our understanding of the *Act* and in working with health information custodians to ensure compliance in their daily practice, we still have a long way to go. It also reinforced the need for health information custodians to not only familiarize themselves with my office's orders but to amend their business practices to comply with the concrete guidance contained therein.

This is one reason why I strongly believe that the creation of a "Best Practice" will go a long way in assisting health information custodians to securely destroy their records. We will be publishing this jointly with NAID and CML, and will be releasing it at NAID's Annual Conference on October 29, 2009.

In the meantime, let us bring to an end any future health records "blowing in the wind." Clearly, we know better than to allow this to happen again.

July 3, 2009

Ann Cavoukian, Ph.D.
Commissioner

Date

Information and Privacy
Commissioner of Ontario

2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8
CANADA

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Email: info@ipc.on.ca
Website: www.ipc.on.ca