PHIPA Order
HO-011

October 13, 2011

Information & Privacy Commissioner,
Ontario, Canada

Ann Cavoukian, Ph.D.
Commissioner

**Information and Privacy Commissioner,
Ontario, Canada**

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

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Web site: www.ipc.on.ca

Table of Contents

EXECUTIVE SUMMARY 1

1.0 BACKGROUND 3

2.0 SUMMARY OF CONCLUSIONS 3

3.0 THE INCIDENT 4

3.1 Cancer Care Ontario 4

3.2 ColonCancerCheck Program 5

3.3 The Screening Reports 7

3.4 The Pilot 7

3.5 The Consultant's Report 9

3.6 The December 23, 2010 Privacy Impact Assessment 11

3.7 Transfer of Screening Reports 13

3.8 The Breach and CCO's Response 15

3.9 Containment and Notification 16

4.0 CONDUCT OF THE INVESTIGATION 17

5.0 ISSUES ARISING FROM THE INVESTIGATION 18

6.0 RESULTS OF INVESTIGATION 18

7.0 ORDER 34

EXECUTIVE SUMMARY

Organizations subject to the *Personal Health Information Protection Act* (the *Act*) that implement programs involving personal health information must ensure that those programs are designed to reflect *evolving* privacy and security standards. In addition, those organizations are required to be vigilant in ensuring that their existing practices and procedures *continue* to protect privacy and *continue* to maintain the confidentiality of the personal information in their custody and control, in light of evolving standards.

The present Order relates to an initiative of Cancer Care Ontario (CCO) that involved the delivery of Screening Reports to over 7,000 physicians in Ontario. Each of the Screening Reports included the personal health information of large numbers of patients.

On June 27, 2011, the Office of the Information and Privacy Commissioner of Ontario (IPC) was advised by representatives of CCO that a number of packages which included Screening Reports were unaccounted for, and believed to have been lost by Canada Post Corporation (Canada Post). These packages were sent via Canada Post's Xpresspost courier service for delivery to the physicians of individuals who were participating, or eligible to participate, in the ColonCancerCheck program (CCC).

I immediately initiated an investigation into this serious breach of the *Act*. As part of the investigation, my staff advised CCO on the steps that it should be taking to contain the incident and to notify affected individuals. In the interim, CCO agreed that it would not send out any further Screening Reports containing the health information of Ontarians.

My investigation determined that CCO had not taken the steps that were reasonable in the circumstances to ensure the secure transfer of the records of personal health information contained in the Screening Reports. Accordingly, I found that CCO did not put into place practices and procedures to protect the privacy of individuals whose health information it had received, and it did not maintain the confidentiality of that information, contrary to its obligations under the *Act*. In particular, I found that CCO had available to it more secure, electronic options for the transfer of the screening reports to physicians. Thus, the alternative, of sending the Screening Reports to physicians in paper format, was unacceptable.

In addition, CCC had a *Privacy Breach Management Procedure* in place that had been approved by my office in 2008. The procedure requires staff to immediately report any privacy breaches, suspected privacy breaches, and/or privacy risks that may lead to a privacy breach, to the CCC Privacy Specialist or to the CCO Chief Privacy Officer. While CCC staff were alerted on April 26, 2011 that three physicians working in one office had not received their Screening Reports affecting 2,388 individuals, it was not until June 1, 2011 that staff advised the CCC Program Manager and CCO's Privacy and Access Office of the issue. As a consequence of this failure to follow their own stated procedure, delays were incurred in responding to the breach. This affected CCO's ability to contain the breach and conduct their investigation in a timely and efficient manner.

Days before the release of this Order, CCO advised me that it had decided to develop its own web portal for the next delivery of Screening Reports.

Based on the findings made in this investigation, and in light of the decision of CCO to develop its own web portal for the next delivery of Screening Reports, I have ordered CCO to take a number of actions, including:

- Discontinue the practice of transferring Screening Reports containing personal health information to physicians in paper format;
- Provide a full report to my office on the advantages and disadvantages of transferring the Screening Reports in electronic format via the existing OntarioMD web portal, as compared to their proposed new CCO web portal. This report is to include a complete assessment of the security and privacy protective measures that will be built into the architecture of the proposed CCO web portal and should compare those measures with the security and privacy protective measures of the OntarioMD web portal. CCO must obtain the approval of my office prior to resuming the transfer of Screening Reports to Primary Care Physicians.
- Review the *CCC Privacy Breach Management Procedure* and any related policies and procedures to clarify and ensure that those having an employment, contractual or other relationship with Cancer Care Ontario are fully aware of their responsibility to immediately report any privacy breaches, suspected privacy breaches and/or privacy risks to appropriate individuals at Cancer Care Ontario with responsibility for privacy issues.
- Conduct additional training with those having an employment, contractual or other relationship with Cancer Care Ontario to ensure that they are fully aware of their duties and responsibilities under the *CCC Privacy Breach Management Procedure*.

1.0 BACKGROUND

On June 27, 2011, the Office of the Information and Privacy Commissioner of Ontario (IPC) was advised by representatives of Cancer Care Ontario (CCO) that a number of packages which included the health information of a large number of Ontarians were unaccounted for and were believed to have been lost by Canada Post Corporation (Canada Post). These packages were sent via Canada Post's Xpresspost courier service for delivery to Primary Care Physicians (PCPs) of individuals who were participating, or eligible to participate, in the ColonCancerCheck program (CCC). The packages contained information derived from the colorectal cancer screening registry compiled and maintained by CCO and included Screening Reports, which will be described later in this Order.

The IPC commenced an investigation into the incident. As part of the investigation, my staff advised CCO on the steps that it should take to contain the incident and on notification of affected individuals. In the interim, CCO agreed that it would not send any further Screening Reports containing the health information of Ontarians, pending the completion of this investigation.

Based on information gathered during the initial stages of my investigation, and in light of the significant number of individuals affected by this incident, I decided that this matter warranted a full review under the *Personal Health Information Protection Act, 2004* (the *Act*).

2.0 SUMMARY OF CONCLUSIONS

I conclude that in the circumstances of this review, CCO did not take steps that were reasonable in the circumstances to ensure the secure transfer of the records of personal health information of individuals whose information was contained in the Screening Reports. Accordingly, CCO did not put into place practices and procedures to protect the privacy of individuals whose personal health information it had received, and maintain the confidentiality of that information, contrary to its obligations under section 13(2) of Regulation 329/04 to the *Act* (the Regulation). In particular, I find that CCO had available to it more secure, electronic options for the transfer of the Screening Reports to PCPs. Therefore, the alternative, of sending the Screening Reports to PCPs by courier in paper format, was unacceptable.

In addition, CCC had a *Privacy Breach Management Procedure* in place that had been approved by my office in 2008. The procedure requires staff to immediately report privacy breaches, suspected privacy breaches and/or privacy risks that may lead to a privacy breach to the CCC Privacy Specialist in person, by email or by telephone. An option is also provided to report privacy breaches, suspected privacy breaches and/or privacy risks to the CCO Chief Privacy Officer when a staff member is not comfortable making the report to the CCC Privacy Specialist.

As set out in detail below, CCC Call Centre staff were alerted on April 26, 2011 that three physicians working in one office had not received their Screening Reports affecting 2,388 individuals. It was not until June 1, 2011 that staff advised the CCC Program Manager and

CCO's Privacy and Access Office that a problem might exist. As a consequence of this failure to follow the procedure, delays were incurred in responding to the breach. This affected the ability of CCO staff to contain the breach and to conduct their investigation in a timely and efficient manner. This in turn also caused delays in the notification of affected individuals.

3.0 THE INCIDENT

3.1 Cancer Care Ontario

CCO is an agency of the Ontario government, funded through the Ministry of Health and Long-Term Care (the Ministry). Its mandate includes the development of "…cancer prevention and screening programs designed to reduce cancer risks and raise screening participation rates."

Pursuant to section 13(1) of the Regulation, CCO is a "prescribed person" in respect of the Ontario Cancer Screening Registry, formerly known as the Colorectal Cancer Screening Registry. The CCC is a component of the Ontario Cancer Screening Registry.

As a prescribed person, the practices and procedures put in place by CCO for the purpose of protecting the privacy of the individuals whose personal health information it receives and maintaining the confidentiality of the personal health information are subject to approval by my office on a triennial basis. If approval is granted, and assuming that all other requirements in the *Act* and the Regulation are met, CCO has the authority to collect personal health information from health information custodians and to use and disclose this personal health information for the purposes of facilitating or improving the provision of health care, and for other purposes permitted by the *Act* and the Regulation, without the consent of the individuals to whom the personal health information relates. Correspondingly, section 39(1)(c) of the *Act* gives health information custodians the authority to disclose personal health information to CCO for the purposes of facilitating or improving the provision of health care.

The requirement that CCO put in place practices and procedures for the purpose of protecting the privacy of the individuals whose personal health information it receives, and for maintaining the confidentiality of that personal health information ("practices and procedures"), and that these practices and procedures be reviewed and approved by my office every three years, is set out in section 13(2) of the Regulation. A further requirement that CCO make a plain language summary of its practices and procedures publicly available is set out in section 13(3) of the Regulation.

Pursuant to these provisions, my office's approval of CCO's practices and procedures is a precondition to its ability to collect, use and disclose personal health information in accordance with the *Act* and the Regulation. I initially approved the practices and procedures of CCO in respect of the CCC on an interim basis on May 1, 2008. However, to synchronize the timing of the reviews of all prescribed persons under the *Act*, this approval only remained in effect until October 30, 2008. On October 31, 2008, the practices and procedures of CCO in respect

of the CCC were approved for a three-year period, until October 30, 2011. My letter dated October 31, 2008, approving the practices and procedures of CCO, stated:

> Based on a review of practices and procedures submitted, I am satisfied that Cancer Care Ontario in respect of the Colorectal Cancer Screening Registry continues to have practices and procedures in place for sufficiently protecting the privacy of individuals whose personal health information it receives and for sufficiently maintaining the confidentiality of that information.

As set out in the approval letter, the practices and procedures that were reviewed and approved by my office in 2008 were those that were in place *at that time*. While this did not preclude CCO from developing and putting into place new practices and procedures or amending the practices and procedures previously approved by my office prior to the next scheduled review in 2011, any review of the new or amended practices and procedures by my office would not occur until the next scheduled review in 2011, unless my office was specifically asked by CCO to conduct such a review or unless a formal review was conducted pursuant to Part VI of the *Act*.

Given this, it is important to note at the outset that the incident under review in this Order did not stem from a practice or procedure reviewed by my office in 2008. I will discuss this further, in greater detail, later in this Order.

3.2 ColonCancerCheck Program

As noted above, the ColonCancerCheck Program (CCC) is one of CCO's screening initiatives. The program is a component of the Ontario Cancer Screening Registry referred to in section 13(1) of the Regulation. CCC was established in 2007 in part to expand access to colorectal screening and to support physicians and other health providers in their efforts to ensure appropriate and timely colorectal cancer screening takes place.

CCO has provided the following background information about the CCC:

> The program structure of CCC allows at risk populations within Ontario to receive information about the advantages of early screening for colorectal cancer. Entry into CCC can be [made] from multiple access points, including the following:
>
> - PCPs – CCC sent letters to eligible attached patients [i.e. those with a PCP] directing them to participate in screening through their PCPs;
> - Pharmacists – unattached patients [i.e., patients without a PCP] could obtain information about CCC and access it through a pharmacist;
> - Telehealth Ontario – unattached patients could obtain information about CCC and access it through Telehealth Ontario; and
> - Public Awareness Campaigns.

> All Ontarians 50 years of age or older who did not have a family history of colorectal cancer or were asymptomatic were invited by CCC to be screened every two years. CCC identified these individuals through its analysis of [personal health information] collected from the [Ministry], labs, and hospitals, as well as from other CCO programs. Eligible individuals were provided with CCC-branded Fecal Occult Blood Test ("FOBT") kits, which included easy-to-read and understand instructions and a postage-paid envelope. An individual could mail or drop off the completed test kit at a participating laboratory. The kit included a privacy insert with information concerning the manner in which an individual's [personal health information] was collected, used and disclosed by CCC.

Initially, a number of individuals were invited to join the CCC by letter and, after the first year of operation, additional eligible individuals were also contacted by letter. These invitations were sent via regular mail using the Canada Post mail service. Subsequent communications with individuals about their participation in the CCC were also sent via mail. Given the volume of correspondence with individuals, CCO used a third party service provider to assist with the mailings. These mailings were the subject of a Privacy Impact Assessment that was reviewed by my office (the 2008 PIA), and formed part of the practices and procedures that were reviewed and approved by my office in 2008. Consequently, the practice of communicating with *individuals* via mail in order to send individual invitations and test results was approved by my office as part of our review in 2008.

As part of the CCC, information was collected by CCO and a registry database was maintained relating to the following:

- eligible population,
- invited population,
- participating population,
- results of screening tests,
- recalled/reminded population,
- participant activity, and
- dispensing of FOBT kits.

The 2008 PIA stated that after the first year of operation, CCO "may" provide personal health information for "decision-support tools" to PCPs about their patients who were participating in the CCC. In particular, page 14 of the 2008 PIA states:

> In future years, past 2008/2009, CCO, the prescribed registry, *may provide [personal health information] for decision-support tools related to the CCC to PCPs about their rostered patients.* For example, a PCP may be provided with a listing of their patients who are due for an FOBT. This PIA Report does not cover PCP reporting. [Emphasis added.]

The 2008 PIA did not specifically mention Screening Reports, which are the subject of this review. Further, the provision of personal health information to PCPs for "decision-support tools" was only mentioned as a possibility. The 2008 PIA also did not indicate how "decision-support tools" would be transferred to the PCPs. In fact, the 2008 PIA specifically states "[t]his PIA Report does not cover PCP reporting."

3.3 The Screening Reports

Subsequent to the 2008 approval of its practices and procedures by my office, CCO developed a plan for the delivery of Screening Reports to PCPs, the reports that were eventually the subject of the breach at issue in this Order. While CCO refers to these reports as SARs in its representations, in this Order, they are referred to as the Screening Reports.

According to CCO, the purpose of the Screening Reports is to increase screening rates by providing up-to-date information to PCPs on the status of their patients. The Screening Reports allow PCPs to identify patients who have been screened, patients who are eligible to participate but have not yet been screened, patients who require follow-up, and the nature of that follow-up. The reports enable PCPs to track and improve their screening rates and facilitate appropriate and timely follow-up.

These Screening Reports included an "all patients" list which sets out the names of patients enrolled in the CCC Program, and the names of those not enrolled, but eligible for enrolment, and included: patients' ages, addresses, status' in the CCC, health numbers, FOBT and/or colonoscopy test results; and details regarding dates and types of screening eligibility. The Screening Reports also included aggregate data such as the number of patients who were eligible for screening, the number who had completed screening tests and the PCPs' estimated progress towards financial incentives for screening tests. They also provided snapshots of the target screening population and allowed the PCP to compare his or her screening rates with other PCPs in their Local Health Integration Networks and in the province.

CCO advised that the Screening Reports did not contain new health information that PCPs did not already have. This means that PCPs would have already received this information through other sources. The failure to receive these Screening Reports did not mean that the PCPs were missing any clinical information that they should have had for the purposes of providing health care. The Screening Reports simply compiled the information that would facilitate the required follow-ups and provided additional aggregate data on the PCPs' screening performance.

3.4 The Pilot

The Screening Reports were initially implemented as a pilot project that CCO refers to as the Invitation and Reporting Pilot (the Pilot). CCO states:

> The scope of the Pilot included the assessment of two reinforcing strategies – participant invitations and provider reports. These strategies were built to take

advantage of existing technology within the program to facilitate screening, improve patient care and increase the screening participation for colorectal cancer thereby allowing CCC to enhance the population-based components of the program and to better support PCPs with knowledge based tools.

According to CCO, the Pilot was conducted between April 2009 and February 2010 and involved the participation of 120 PCPs. Two methods were used for the delivery of the Screening Reports to the PCPs. A Screening Report was printed and delivered via courier to each PCP, and the same Screening Report was made available to that PCP through the OntarioMD web portal.[1]

The OntarioMD web portal is an internet website used by physicians to access and share clinical tools and resources, including tools for collaboration with other physicians. The web portal is an initiative of OntarioMD, established by the Ontario Medical Association and the Ministry to assist physicians in implementing information technology to improve patient care and practice efficiency, including making the transition from paper records to electronic medical records.

The PCP addresses used for the courier delivery of the Screening Reports in paper format and the USB drives were obtained from a Ministry database.

CCO indicated that the CCC Senior Privacy Specialist provided consultation and support to the Pilot by:

- Participating in the development of a privacy impact assessment in respect of the privacy risks associated with the Pilot;
- Providing input to the design of business rules;
- Defining privacy business requirements for the project;
- Assessing processes to ensure appropriate privacy controls were embedded;
- Supporting the discussions with OntarioMD for the development of an online portal for physician access to [their patients' personal health information].

A Privacy Impact Assessment dated June 5, 2009 (the 2009 PIA) was prepared to identify the privacy risks associated with changes to the CCC since the 2008 PIA, including implementation of the Pilot.

The 2009 PIA focuses on the privacy risks associated with failing to establish relationships with all third parties providing services on behalf of CCO in respect of personal health information in the Pilot. It also focuses on ensuring that no more personal health information is being collected, used and disclosed by CCO than is reasonably necessary and that all collections, uses and disclosures of personal health information comply with the *Act* and the Regulation.

1 The Pilot also involved the transfer of a patient validation tool, which included personal health information, to participating PCPs. The main purposes of the validation tool were to identify patients who were eligible to receive an invitation letter for screening and to verify their address information. This tool was stored on encrypted USB drives that were sent by courier to the PCPs.

The 2009 PIA did not include a detailed discussion of the methods by which the Screening Reports would be transferred to PCPs, nor did it address the privacy risks associated with the chosen methods.

In addition, the CCC "Privacy Impact Assessment - Risk Register" related to the 2009 PIA does not identify any privacy risks associated with the chosen methods of transferring the Screening Reports to PCPs.

3.5 The Consultant's Report

To assist CCO in the evaluation of the Pilot, it retained the services of a consulting firm which prepared a report entitled "ColonCancerCheck Invitation Pilot Assessment Report," dated February 26, 2010 (the Consultant's Report).

The Consultant's Report sets out the Consultant's findings regarding the effectiveness of the Pilot and the usefulness of the data in the Screening Reports for PCPs. In this regard, the Consultant's Report confirmed that the Screening Reports had great value to PCPs.

Of significance to this review, the Consultant's Report also contained findings regarding the methods that were used to transfer the Screening Reports to PCPs. One of the key findings in relation to the OntarioMD web portal was as follows:

> A limited number of physicians accessed their report online through OntarioMD due to challenges with log on access, inability to remember the two passwords required as well as a general preference for having a paper copy. Opportunity exists to increase the number of physicians that access their report online by simplifying the access process, ensuring it is easy to download and print and by potentially forcing online access by not providing a paper copy. A clearly defined service agreement is required with a partner organization to ensure that physicians are provided with a clean and smooth experience.

While this finding notes a problem with log on access to the OntarioMD web portal, in the body of the Consultant's Report the Consultant states that CCO was not aware that some of the participating PCPs did not have an OntarioMD user identification that would have given them access. In particular, the Consultant's Report states:

> [CCO] was not aware at the time that Pilot participants without an [OntarioMD] user ID could not be granted access but rather needed to request access after their user ID was created. A total of 31 participants did not have user IDs. The lack of access rights was identified after a total [of] five physicians phoned the support line to indicate that they could not view the logo. Once the issue was highlighted, it was addressed immediately, but it is likely that this problem resulted in a number of physicians who otherwise would have [,] not accessing their report online. Exact numbers cannot be measured.

Also, while some PCPs recognized the value in an electronic version of the Screening Report, they preferred using the paper format since that option had been made available to them as well. The Consultant's Report suggests that the impact of these issues on the numbers of PCPs who would otherwise have used the OntarioMD web portal could not be determined.

Section 10.2 of the Consultant's Report also contains a crucial assessment of the transfer of the Screening Reports to PCPs, in paper format via courier. Under the heading *Privacy Considerations*, the Consultant's Report stated:

> Some privacy considerations were raised in terms of the means by which the [Screening Report] was distributed. When contacted for feedback on the [Screening Report] one physician informed CCC that he did not receive the [Screening Report]. After some investigation, it was discovered that the [Screening Report] had been signed for by a temporary staff and had been placed in a different suite. Although it was successfully returned to the physician unopened, ***this incident further highlights the risks involved in sending personal health information through insecure channels and via paper.*** [Emphasis added.]

This note of caution was repeated in the *Key Findings*, also found in Section 10.2 of the Consultant's Report:

> Distribution of the paper lists required a significant amount of time and work and effort indicating a ***need to investigate pushing physicians to a secure portal to retrieve the [Screening Report] and print for themselves. This would ensure that privacy best practices were met.*** [Emphasis added.]

In commenting on this section of the Consultant's Report, CCO states the following:

> The [Consultant] found that this incident highlighted the risks involved in sending [personal health information] via courier and recommended that further consideration was required regarding (a) how to ensure paper was to be safely delivered and (b) how to lessen the use of paper tools. The Pilot report contained conflicting statements as to whether the delivery of a paper version of the [Screening Report] by courier would ensure that "privacy best practices" were met. The CCC Senior Privacy Specialist provided consultation and support to the pilot in considering privacy risks associated with different delivery methods.
>
> The [Consultant] ultimately recommended that going forward, [Screening Reports] should be delivered through an improved web portal that provided PCPs with a "seamless experience" in receiving and utilizing the data products provided by CCO. In order to reduce the manual work effort imposed on CCO in producing paper copies of the [Screening Report], the [Consultant] recommended that [Screening Reports] should not be printed and couriered but instead should be available online through the improved web portal.

The essence of the CCO interpretation of the Consultant's Report findings is that the recommendation to use a web portal for the transfer of the Screening Reports to PCPs was not based on any privacy risk associated with the decision to deliver the Screening Reports in paper format via courier. Rather, the finding was said to be based on the administrative efficiencies involved in the proposed electronic transfer of the Screening Reports to PCPs. Clearly, that was only one of the risks identified.

CCO's interpretation of the Consultant's Report is not at all reasonable. While I agree that the Consultant's Report identified administrative conveniences associated with the transfer of the Screening Reports through a web portal, it specifically noted that there were indeed privacy risks associated with the transfer of paper Screening Reports to PCPs via courier. This is critical since this comprehensive evaluation of the Pilot appears to be the first time that anyone acting for or on behalf of CCO identified and addressed the privacy risks associated with the transfer of Screening Reports in paper format via courier. As I set out below, another privacy impact assessment was done in December of 2010. However, prior to December of 2010, it appears that CCO did not conduct a separate evaluation of the privacy risks associated with the transferring of the Screening Reports in paper format via courier.

In my view, there is only one reasonable way in which to interpret the findings of the Consultant's Report – namely, that the Consultant hired by CCO clearly identified the privacy risks associated with the delivery of the Screening Reports in paper format, via courier. Given that there were only 120 participating PCPs in the Pilot and one package containing Screening Reports had already been misplaced, there was sufficient evidence to reasonably anticipate that delivery of the Screening Reports in paper format via courier would result in at least some of the Screening Reports going astray.

3.6 The December 23, 2010 Privacy Impact Assessment

Based on the overwhelmingly positive response of participating PCPs to the Pilot, CCO decided to proceed to issue Screening Reports to approximately 7,600 PCPs in Ontario. A privacy impact assessment was completed in December of 2010 (the 2010 PIA) to assess changes that had been made to the CCC since the 2009 PIA, including the transfer of Screening Reports to PCPs. The 2010 PIA states:

> The [Screening Report] will be couriered to PCP by the fulfillment house [sometimes referred to as a mail forwarding house which offers printing and mail management services]. CCC will produce [the Screening Report] in a PDF format and transfer the report to fulfillment house for mailing via a secure File Transfer Protocol (FTP) – [named]. ***Due to time constraint, the portal solution, which was in place for the invitation pilot for delivery of [Screening Reports] to PCPs is not feasible.*** CCC will also be sending a pre brief letter to PCP to provide them a notice on the upcoming report. The pre-brief letters will be mailed on January 28th, 2011. The pre-brief letter will also contain a section on frequently asked questions, including privacy related questions. [Emphasis added.]

The 2010 PIA noted that the Screening Reports were to be sent to PCPs via courier in "three waves." **It also noted that couriering the Screening Reports to the wrong address would result in a privacy breach** and that avoiding such a result was dependent on the accuracy of the sources of the address information provided by the Ministry. The 2010 PIA also noted, without clarifying whether it was referring to regular mail or courier delivery, that the "breach rate" from its "mailings," had been minimal – 0.01% of the total. It also stated:

> There is also a risk of breach if [the Screening Report] is delivered to wrong address. The risk is being mitigated by sending [the Screening Report] via a courier requiring the individual named on the package to sign it in order to receive the package. As well[,] [the Screening Report] will not be mailed to any addresses that fulfillment house finds not mailable during the address validation process. Also, fulfillment house will not mail the report packages to addresses from which the pre brief letter was returned as undeliverable.
>
> Mitigating Strategy
>
> **The CCC Program should investigate possibility of providing [Screening Reports] to physicians via portal for the next release scheduled for September 2011.** [Emphasis added.]

In the CCC Risk Register relating to the 2010 PIA, the following risks and recommendations were identified:

> **Risk 4: There is a risk of privacy breach if the package was delivered at the wrong address.**
>
> **Recommendation 5:** The [Screening Reports] will be couriered to physicians address requiring signature by the receiving party. The [Screening Reports] will not be sent to addresses that returned the pre-launch letter or to the addresses which will be classified as not mailable by the fulfillment house.
>
> **Recommendation 6:** ***The CCC Program should ensure that privacy escalation process is in place for any potential breach calls received from physicians and patients.***
>
> **Recommendation 7:** ***The CCC program should investigate possibility of providing [Screening Reports] to physician via portal for the next release scheduled for September 2011.*** [Emphasis added.]

Based on my review of the 2010 PIA, and the related CCC Risk Register, three observations can be made. First, CCO clearly identified the privacy risks associated with sending paper copies of the Screening Reports via courier to participating PCPs. This included the possibility that Screening Reports could be delivered to the incorrect address. Second, CCO recognized the need for additional vigilance in identifying potential privacy breaches that could arise. Third, the desirability of using a web portal was again noted, presumably to provide for a more secure

transfer of the Screening Reports to PCPs, as well as improving the administration of the CCC. These three observations will factor into my analysis as to whether CCO met its obligations under section 13(2) of the Regulation.

3.7 Transfer of Screening Reports

To facilitate the delivery of the Screening Reports to PCPs in paper format via courier, CCO contracted the services of the Lowe Martin Group (LMG), a fulfillment house, also referred to as a mail forwarding service provider, offering printing and mail/courier management services. The relationship between LMG and CCO is governed by a series of agreements.

The parties entered into an agreement dated April 25, 2008 that governs their relationship, including the services and service levels that LMG was to provide, and the obligations of LMG in respect of the collection, use and disclosure of personal health information. It was subsequently amended effective August 31, 2009 to extend the term to August 31, 2010. Another extension was agreed to effective December 6, 2010, which extended the agreement between the parties to September 2, 2011.

CCO and LMG entered into a new Services Agreement effective April 11, 2011. Schedule A of that agreement provided that shipments were to be made using an "optimal carrier based on agreed variables of delivery time and costs." Schedule B of the agreement, titled "Principles and Procedures for the Provision and Use of Personal Information and Personal Health Information," required LMG to comply with detailed requirements concerning the collection, use, disclosure and destruction of personal health information.

CCO also stated that it established the specific terms of LMG's involvement in the production and delivery of the Screening Reports in a *CCO SAR Project Brief* dated January 25, 2011. The CCO *SAR Project Brief* includes additional and more specific terms and conditions relating to the transfer of the Screening Reports; it also confirmed that there would be two "mailings" to PCPs.

The initial mailing was described as the *SAR Briefing*. It included an introductory letter and a Frequently Asked Questions pamphlet about the Screening Report and the CCC. There was no health information in the *SAR Briefing*. The *SAR Briefing* was to be delivered via regular mail to all participating PCPs with addresses obtained from the Ministry database that "passed the Canada Post Address Validation Process."

In order to ensure the accuracy of the PCPs' address information, the *SAR Briefing* letters were tagged with sequential numbers to enable the tracking of returns. Any mail returned as undeliverable was to be tracked by LMG and scanned into a separate report that would be sent to CCO on a weekly basis. The Screening Reports were to be sent in the second phase. All of the returned *SAR Briefing* letters were to be removed from CCO's mailing list so that the second planned mailing, which would include the Screening Reports, would be sent only to those PCPs for whom the *SAR Briefing* was not returned.

It was agreed that LMG would print the necessary materials and prepare packages containing the Screening Reports for those PCPs who remained on the mailing list, after having accounted for returned mail from the initial *SAR Briefing* mail out.

In accordance with the plan set out in the 2010 PIA, the Screening Reports were sent in three waves: 200 Screening Reports were sent during the week of February 28, 2011; 3,006 Screening Reports were sent during the week of March 15, 2011; and 3,745 Screening Reports were sent during the week of March 22, 2011. Unlike the *SAR Briefing*, these Screening Reports contained personal health information. The number of individuals whose health information was contained in each Screening Report varied. For example, some of the Screening Reports contained the health information of approximately 300 patients, while others contained information relating to more than 1,300 patients.

CCO stated that the Screening Reports were to be sent using Canada Post's Xpresspost courier service "with signature required." I note that Canada Post refers to this service as "Xpresspost Certified" and LMG describes the service as "Canada Post Xpresspost Standard service with Signature required." Generally, there appears to be agreement among the parties as to the service to be provided. CCO states that the Xpresspost terms of service required Canada Post to deliver the packages overnight, track the delivery of each package, obtain a signature of an adult representative of the PCP upon delivery (absent certain exceptional circumstances), and return any undeliverable packages to LMG for destruction. Regarding the requirement to obtain a signature, CCO stated:

> Canada Post was generally required to obtain a signature upon delivery from an adult representative of the PCP. However, if the representative refused to provide a signature, Canada Post's delivery agent would ask the representative to print his or her name in block letters. If the representative refused to print his or her name, the delivery agent would deliver the [Screening Report] package and indicate that the [Screening Report] package was delivered with signature refused on Canada Post's tracking system.

However, as to the requirement for a signature on delivery, Canada Post stated:

> If the addressee refuses to sign for the item…the item will be sent back (Return to Sender) to the original sender. This means that either a signature is obtained or the package is returned, no alternatives are contemplated.

Canada Post explained that the Xpresspost courier service allows for tracking via the recording of scanning events that are logged in its Event Manager system. During shipment preparation, each parcel is assigned a tracking number and parcels are then scanned as they move through the delivery network.

Canada Post also explained that each parcel scanning and tracking event is logged into the online system and customers are able to access this information to determine the status of their shipments. Canada Post stated that their system includes a function which allows customers to

view and print a "Delivery/Confirmation Certificate" once the parcel is delivered. As well, the signature may be viewed online.

It appears that despite the fact that the 2010 PIA indicated that the PCPs would be contacted to confirm receipt of the first wave of packages containing the Screening Reports, no such steps were taken by CCO. Consequently, CCO would only know if there was a problem with delivery if the package containing the Screening Reports was returned to LMG as undeliverable, or if someone called to advise CCO that a PCP had not received his or her package. In other words, CCO was relying primarily on the return of undelivered Screening Reports to LMG for destruction as the primary method for determining the delivery status of the packages containing the Screening Reports, instead of proactively confirming receipt, as originally intended.

3.8 The Breach and CCO's Response

On April 26, 2011, the CCC Call Centre received a call staff in a physicians' office indicating that they had not received the Screening Reports for three physicians in that practice. The Call Centre noted the undelivered status within CCC's customer relationship management application and forwarded a delivery confirmation request to LMG for investigation. These three Screening Reports contained the health information of 2,388 individuals.

On April 28, 2011, LMG asked Canada Post to conduct a trace on the three Screening Reports. LMG states that Canada Post informed it that it could take five to ten business days to conduct the trace. On the same day, LMG informed CCO that the online tracking system showed the three Screening Reports to be undelivered.

While there is some dispute between LMG and Canada Post as to the details of the actions taken by each of them following the initial report of the three undelivered Screening Reports, it is clear that some efforts were made by LMG and Canada Post to determine the whereabouts of the Screening Reports between April 28, 2011 and June 1, 2011.

CCO reports that on May 30, 2011, the CCC Call Centre informed "the [Screening Report] working group" of the problem with the three Screening Reports and at that time, this group recommended that the matter be escalated to the CCC Program Manager.

On June 1, 2011, the CCC Program Manager was notified of the issue and CCC in turn notified CCO's Privacy & Access Office of the potential breach that day. The CCO's Director of Privacy & Access requested that CCC determine the total number of patient records contained in the three missing Screening Reports. CCO's Chief Privacy Officer was notified on June 2, 2011.

Efforts to trace the location of the three Screening Reports continued between June 1 and June 14, 2011. On June 14, 2011, Canada Post declared the three Screening Reports lost and CCO's Privacy and Access Office began its investigation.

In response to the three missing Screening Reports, CCO staff met with LMG on June 16, 2011 and requested confirmation of delivery of all Screening Reports to determine the scope of the breach.

On June 17, 2011, CCO began the task of tracing the Screening Reports sent in the third wave, which occurred during the week of March 22, 2011, via Canada Post's online tracking system. CCO staff entered each package tracking number into Canada Post's online tracking system to identify the status of delivery for each Screening Report package couriered during the week of March 22, 2011.

The online tracking system for the Screening Reports sent in waves one and two during the weeks of February 28, 2011 and March 15, 2011, respectively, was unavailable. As explained in an email dated June 17, 2011 between LMG and Canada Post, the ability to use the online system expired 90 days after the Screening Reports were couriered.

On June 22, 2011, Canada Post provided CCO with a status report regarding the 6,951 Screening Reports couriered in all three waves. It stated that 185 packages of Screening Reports appeared not to have been delivered or were not showing as having been delivered by the tracking system.

CCO states that LMG informed it that 63 of the 185 packages of Screening Reports had been deemed undeliverable and had been returned to and had been destroyed by LMG, leaving the total number of unaccounted for packages at 122.

On June 24, 2011, CCO began telephoning the 122 affected PCP offices to determine if the Screening Reports had in fact been delivered.

As noted above, on June 27, 2011, CCO advised the IPC that Canada Post was not able to confirm that a number of the Screening Reports were received by the intended PCPs. It also advised that it continued to work with LMG and Canada Post to determine the status and location of the Screening Reports.

3.9 Containment and Notification

As of July 7, 2011, 41 packages of Screening Reports containing the health information of 20,064 patients were unaccounted for. At the request of the IPC, CCO met in person with each PCP for whom it was not able to confirm delivery. These site visits were conducted by CCO staff beginning on July 13, 2011 and ending on August 10, 2011.

As a result of these site visits, it was discovered that some of the unaccounted for Screening Reports had been delivered to the PCP offices but staff in those offices had either misplaced the packages or had not informed the PCPs of their delivery. As a result of these visits, the number of unaccounted for Screening Reports was reduced from 41 to 17 and the total number of individual patients affected was correspondingly reduced from 20,064 to 7,130.

The IPC worked with CCO to develop PCP and patient notification letters, Frequently Asked Questions for PCPs and patients that were subsequently posted on the CCO web site, and a media release notifying the public of the privacy breach. The media release and notification documents included contact information for CCO and the IPC, for individuals seeking more information or wishing to make a complaint.

On July 26, 2011, CCO released a media statement notifying the public of the incident and began to embark on the process of notification.

4.0 CONDUCT OF THE INVESTIGATION

Section 58 of the *Act* reads:

> (1) The Commissioner may, on his or her own initiative, conduct a review of any matter if the Commissioner has reasonable grounds to believe that a person has contravened or is about to contravene a provision of this Act or its regulations and that the subject-matter of the review relates to the contravention.
>
> (2) Upon deciding to conduct a review under this section, the Commissioner shall give notice of the decision to every person whose activities are being reviewed.

Based on the circumstances set out above, I concluded that there were reasonable grounds to believe that CCO had contravened the *Act* and the Regulation. I therefore decided to conduct a review pursuant to section 58 of the *Act*.

As a result, my office issued a Notice of Review to CCO in accordance with section 58(2) of the *Act*. CCO was invited to make submissions on the facts and issues set out in the Notice of Review as well as any other facts and issues that CCO believed were relevant to the matters under review. In these submissions, CCO was also asked to include a statement of all relevant facts and issues, and reference and provide copies of all relevant legislative provisions as well as all relevant CCO policies, procedures, standards and practices and any documents or other evidence that might be relevant to the review.

Under cover of separate correspondence, my office invited LMG and Canada Post to make submissions relating to the matters under review. The IPC received submissions from CCO, LMG and Canada Post.

5.0 ISSUES ARISING FROM THE INVESTIGATION

(A) Do the Screening Reports contain "personal health information" as defined in section 4 of the *Act*?

(B) Is CCO responsible for the actions of LMG and Canada Post in relation to the transfer of the Screening Reports to PCPs?

(C) As a prescribed person, has CCO complied with its obligations under section 13(2) of the Regulation?

6.0 RESULTS OF INVESTIGATION

Issue A: Do the Screening Reports contain "personal health information" as defined in section 4 of the *Act*?

Section 4(1) of the *Act* states, in part:

> 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,
>
> …
>
> (f) is the individual's health number,

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.

The information contained in the Screening Reports is set out above. CCO acknowledged that the Screening Reports contain personal health information and, in the case of the lost Screening Reports, contained the personal health information of 7,130 patients. On that basis, and having reviewed the sample Screening Reports provided to my office, I find that the Screening Reports contain personal health information as defined in section 4 of the *Act* as they contain identifying

information that relates to the physical health of individuals, relates to the provision of health care to individuals, identifies the provider of health care to individuals and contains the health number of individuals.

Issue B: Is CCO responsible for the actions of LMG and Canada Post in relation to the transfer of the Screening Reports to PCPs?

CCO takes the position that Canada Post and LMG were not its "agents" as that term is defined in section 2 of the *Act*. Under the *Act*, the definition of the term refers only to an "agent" of a health information custodian and CCO, in compiling or maintaining the CCC, is a prescribed person under section 39(1)(c) of the *Act*, not a health information custodian.

However, CCO goes on to state that LMG is a service provider whose role is to provide a number of services to CCO, including bulk fulfillment, returned mail management, error management and reporting. Pursuant to its agreement with CCO, LMG was required to comply with detailed requirements relating to the collection, use and disclosure of personal health information. Further, pursuant to its agreement with CCO, LMG was required to acknowledge and agree that in the course of providing services pursuant to the agreement, it will only collect, use, store and transfer personal health information on behalf of CCO and not on its own behalf or for its own purposes. Similarly, CCO also states that Canada Post was not an agent but a service provider. Its role was to provide mail and courier services on an ongoing basis.

It is a fundamental principle of fair information practices that an organization remains accountable for personal information in its custody and control, including personal health information, which has been transferred to a third party for processing. For example, principle 4.1.3 of the Canadian Standards Association Model Code for the Protection of Personal Information, now incorporated into the federal *Personal Information Protection and Electronic Documents Act*, states "an organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing."

Applying this principle, I find that regardless of whether Canada Post and LMG fall under the statutory definition of "agent" or not, given CCO's status as a prescribed person, CCO is fully responsible for the actions of organizations that it selects to provide services on its behalf in relation to personal health information.

In my view, while the statutory definition of "agent" in section 2 of the *Act* may not technically apply in these circumstances, (since it refers to a health information custodian rather than a prescribed person), the term "agent" nonetheless applies more broadly, with respect to holding CCO fully accountable for the actions of the service providers whose services it has contracted.

Issue C: As a prescribed person, has CCO complied with its obligations under section 13(2) of the Regulation?

As noted above, section 13 of the Regulation sets out the obligations of CCO as a prescribed person for the purposes of section 39(1)(c) of the *Act*. In particular, section 13(2) of the Regulation states:

> A person who is a prescribed person for the purposes of clause 39(1)(c) of the Act shall put into place practices and procedures,
>
> (a) that are for the purpose of protecting the privacy of the individuals whose personal health information it receives and for maintaining the confidentiality of the information; and
>
> (b) that are approved by the Commissioner every three years.

To satisfy section 13(2) of the Regulation, two requirements must be met. CCO must put into place practices and procedures that are for the purpose of protecting the privacy of the individuals whose personal health information it receives and for maintaining the confidentiality of the information. In addition, these practices and procedures must be approved by my office every three years.

With respect to its obligations under section 13(2) of the Regulation, CCO states:

> It is our position that CCO has complied with the requirements set out in s. 13(2) of the [Regulation]. First, CCO, acting as a prescribed registry, has put practices and procedures into place for the purposes of (a) protecting the privacy of the individuals whose [personal health information] it has received and (b) maintaining the confidentiality of such [personal health information]…Second, the IPC has approved CCO's practices and procedures as a prescribed registry within the last three years; the most recent approval was on October 31, 2008. In accordance with the clear wording of s. 13(2) of the [Regulation], CCO is in compliance with this provision.
>
> In addition, CCO has put into place specific practices and procedures in respect of the delivery of [Screening Reports] to PCPs to protect the privacy of the individuals whose [personal health information] it has received and to maintain the confidentiality of such [personal health information].

Requirement for Approval of Practices and Procedures in Section 13(2)(b) of the Regulation

I had initially approved the practices and procedures put in place by CCO in respect of the CCC on an interim basis on May 1, 2008. To synchronize the timing of the reviews of all prescribed persons under the *Act*, this approval only remained in effect until October 30, 2008. On October 31, 2008, the practices and procedures of CCO were approved for a three-year period, until

October 30, 2011. My letter dated October 31, 2008, approving the practices and procedures of CCO in respect of the CCC, stated:

> Based on a review of practices and procedures submitted, I am satisfied that Cancer Care Ontario in respect of the Colorectal Cancer Screening Registry continues to have practices and procedures in place for sufficiently protecting the privacy of individuals whose personal health information it receives and for sufficiently maintaining the confidentiality of that information.

As set out in my letter dated October 31, 2008, the practices and procedures of CCO in respect of the CCC that were reviewed and approved by my office were those that were in place *at that time*. The practices and procedures put in place by CCO in transferring Screening Reports to PCPs in paper format via courier were developed and implemented *subsequent* to my approval of the practices and procedures of CCO in respect of the CCC in 2008.

In its submissions, CCO stated that section 13(2) of the Regulation does not require CCO to obtain the approval of my office prior to putting in place new practices and procedures or amending existing practices and procedures in the period between triennial reviews. CCO stated:

> Although s. 13(2) of the [Regulation] provides that CCO's practices and procedures must be approved every three years by the IPC, s. 13(2) does not provide that CCO cannot put a practice or procedure into place unless that practice or procedure has already been approved by the IPC.

CCO further stated that the ongoing development of new practices and procedures was explicitly contemplated at the time my office reviewed and approved the practices and procedures of CCO in respect of the CCC in 2008. In particular, it stated that it was "explicitly contemplated that CCO could develop new practices and procedures on an ongoing basis to address new privacy risks as CCC evolved over time."

I agree that section 13(2) of the Regulation does not require CCO to obtain the approval of my office prior to putting in place new practices and procedures, or amending existing ones in the period between triennial reviews, and that new practices and procedures and amendments may be required with the evolution of a particular program.

My office developed the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* (the *Manual*) for use by prescribed persons and entities in developing new or revising existing practices and procedures. When a prescribed person or entity contemplates putting in place practices and procedures with significant privacy or security risks, consultation with my office is advisable.

Page 18 of the *Manual* requires each prescribed person and entity to develop and implement a policy and associated procedures for the ongoing review of the practices and procedures that it has put in place to determine whether amendments are needed or whether new practices and procedures are required. The *Manual* further recommends that each prescribed person and entity review the practices and procedures put in place on an annual basis. This is important, among

other things, to ensure that the practices and procedures are consistent with evolving privacy standards and best practices and that new privacy risks are adequately identified and addressed. With the development of new technologies, the standard for what constitutes reasonable practices and procedures to protect the privacy of individuals in respect of their personal health information will evolve. Therefore, as technological and other solutions that enhance privacy protection develop and become more readily accessible, these solutions become the new standard.

Page 18 of the *Manual* states:

> In undertaking the review and determining whether amendments and/or new privacy policies, procedures and practices are necessary, the prescribed person or prescribed entity must have regard to any orders, guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario under the *Act* and its regulation; evolving industry privacy standards and best practices; amendments to the *Act* and its regulation relevant to the prescribed person or prescribed entity; and recommendations arising from privacy and security audits, privacy impact assessments and investigations into privacy complaints, privacy breaches and information security breaches. It must also take into account whether the privacy policies, procedures and practices of the prescribed person or prescribed entity continue to be consistent with its actual practices and whether there is consistency between and among the privacy and security policies, procedures and practices implemented.

However, after stating that there is nothing in the *Act* and the Regulation that would prevent CCO from putting in place new practices and procedures or amending existing practices and procedures, CCO states:

> Moreover, s. 13(2) does not provide that at any given time, the CCO must have practices and procedures that are acceptable to the IPC. The IPC's role is limited to determining whether to approve CCO's practices and procedures every three years.

If the CCO position is that the jurisdiction of my office to conduct a review of its practices and procedures is limited to the triennial review and approval process set out in section 13(2) of the Regulation, it is mistaken.

While a prescribed person or entity may put in place new or revised practices and procedures between triennial reviews, my office retains the authority to review new or revised practices and procedures pursuant to Part VI of the *Act,* if there are reasonable grounds to believe that they may contravene section 13 of the Regulation. Further, for the reasons set out above, including evolving privacy standards and best practices, the emergence of new privacy risks and the development of new technologies, my office also retains the authority under Part VI of the *Act* to review the practices and procedures put in place by a prescribed person or entity that were previously reviewed and approved by my office under section 13 of the Regulation, to ensure that these

practices and procedures continue to protect the privacy of individuals whose personal health information it receives, and continue to maintain the confidentiality of that information.

The contention that prescribed persons and prescribed entities are immune from review by my office under Part VI of the *Act*, or that my office is limited to reviewing the practices and procedures put in place by prescribed persons and entities every three years, is untenable and is inconsistent with the privacy protection scheme established by the *Act*.

It is clear that the Legislature did not intend to limit the jurisdiction of my office in this way, to begin with, because it also made the practices and procedures put in place by prescribed persons and entities subject to review and approval by my office, every three years. Prescribed persons and prescribed entities are bound by the *Act* and subject to a review under Part VI of the *Act* in appropriate circumstances, on the same basis that health information custodians and other persons and organizations are subject to review under Part VI of the *Act*. Prescribed persons and prescribed entities do not have a special status to conduct their operations with impunity. CCO's limiting interpretation would have the potential to seriously undermine the purposes of the *Act* as set out in section 1, including the purpose of providing for independent review of complaints with respect to personal health information. I reject this position.

As a result, I am satisfied that while CCO is only obliged to have its practices and procedures reviewed and approved by my office every three years, I have the authority under Part VI of the *Act* to review the practices and procedures put in place by CCO since the time of the review conducted by my office in 2008. This includes the manner in which Screening Reports were transferred to PCPs, and any associated issues raised.

Requirement to Put in Place Practices and Procedures in Section 13(2)(a) of the Regulation

Section 13(2)(a) of the Regulation requires CCO to put into place practices and procedures that are for the purpose of protecting the privacy of the individuals whose personal health information it receives and for maintaining the confidentiality of the personal health information. While the *Act* and the Regulation do not specify the precise nature of the practices and procedures that are to be put in place, in my view, the *Act* and the Regulation require that the practices and procedures be reasonable, having regard to the nature of the information and the activities that are undertaken, and all the surrounding circumstances.

The *Manual* developed by my office requires a prescribed person to develop and implement a policy for the secure transfer of records of personal health information. In particular, the *Manual* provides that policies and procedures must be implemented with regard to the secure transfer of records of personal health information in both paper and electronic format.

The *Manual* requires the policies and procedures regarding the secure transfer of records of personal health information to include the conditions pursuant to which records of personal health information will be transferred, the agent(s) responsible for ensuring secure transfer, the documentation to be completed in relation to secure transfer, the agent(s) responsible for completing the documentation and the required content of the documentation.

In developing policies and procedures regarding the secure transfer of records of personal health information, page 88 of the *Manual* states:

> The prescribed person or prescribed entity must ensure that the approved methods of securely transferring records of personal health information and the procedures and safeguards that are required to be implemented in respect of the secure transfer of records of personal health information are consistent with:
>
> - Orders issued by the Information and Privacy Commissioner of Ontario under the *Act* and its regulation, including but not limited to Order HO-004 and Order HO-007;
> - Guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario, including *Privacy Protection Principles for Electronic Mail Systems and Guidelines on Facsimile Transmission Security*; and
> - ***Evolving privacy and security standards and best practices.*** [Emphasis added.]

While the *Manual* does not specify when records of personal health information should be transferred in paper format and when they should be transferred in electronic format and the method of transfer, the *Manual* states that the prescribed person or prescribed entity must ensure that "the approved methods of securely transferring records of personal health information" are consistent with "*evolving privacy and security standards* and best practices."

Some guidance regarding what constitutes reasonable measures for the secure transfer of records of personal health information, and how privacy and security standards and best practices evolve, can be found in Investigation Report F08-02, a decision of the Information and Privacy Commissioner of British Columbia. That report involved the use of a courier to transmit unencrypted magnetic tapes containing personal health information from New Brunswick to British Columbia. Following the loss of the magnetic tapes, an investigation was conducted.

Section 30 of British Columbia's *Freedom of Information and Protection of Privacy Act* requires public bodies to protect personal information in their custody or control by implementing reasonable security measures to address risks such as unauthorized access, collection, use, disclosure or disposal. It states:

> A public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

Former Commissioner Loukidelis had the following comments to make about the reasonableness standard imposed on public bodies by section 30:

> Section 30 of FIPPA requires a public body to take all reasonable measures to protect personal information under its custody or control. In Investigation Report F06-01, dealing with the provincial government's sale of computer backup tapes containing personal information, I said this about the meaning of "reasonable":
>
> > By imposing a reasonableness standard in s. 30, the Legislature intended the adequacy of personal information security to be measured on an objective basis, not according to subjective preferences or opinions. Reasonableness is not measured by doing one's personal best. The reasonableness of security measures and their implementation is measured by whether they are objectively diligent and prudent in all of the circumstances. To acknowledge the obvious, "reasonable" does not mean perfect. Depending on the situation, however, what is "reasonable" may signify a very high level of rigour.
> >
> > The reasonableness standard in s. 30 is also not technically or operationally prescriptive. It does not specify particular technologies or procedures that must be used to protect personal information. The reasonableness standard recognizes that, because situations vary, the measures needed to protect personal information vary. It also accommodates technological changes and the challenges and solutions that they bring to bear on, and offer for, personal information security.
>
> The nature and level of security will depend on the sensitivity of the information. As was also noted in Investigation Report F06-01:
>
> > The sensitivity of the personal information at stake is a commonly cited, and important, consideration. For example, a computer disk or paper file containing the names of a local government's employees who are scheduled to attend a conference or take upcoming vacation does not call for the same protective measures as a disk containing the medical files of those employees.
> >
> > Sensitivity is a function of the nature of the information, but other factors will also affect sensitivity. For example, the sensitivity of medical treatment information for someone who died 70 years ago is less than for someone who died more recently or is living.

The Commissioner also made the following comments about using a courier service as a mode for transferring personal health information:

> Another s. 30 consideration relates to the method of transferring the personal information. The use of a bonded courier service is, generally, considered to be a reliable method of transporting materials. As with other delivery methods, courier delivery is not infallible and a certain percentage of packages are misplaced or lost. Courier companies and Canada Post can provide shipment tracking mechanisms to track shipments along their journey and offer tracking services to help locate missing packages and assist in their recovery if they do go astray. These features of delivery services can be relevant in assessing the reasonableness of security measures respecting the shipment of personal information.

After reviewing all of the circumstances relating to the transfer of the magnetic tapes, Commissioner Loukidelis made the following findings:

> Considering all of these factors, including the nature of the information involved, the failure to use encryption and the ease with which a tracking policy could have been adopted and implemented, I conclude that the Ministry did not comply with its s. 30 duty to take reasonable security measures to protect personal information against unauthorized disclosure or use.

Although Commissioner Loukidelis found that the use of a bonded courier service was generally considered to be a "reliable method of transporting materials," he also noted that shipment tracking features were relevant in assessing the reasonableness of the security measures used. What is significant for the purposes of this review is that he also found that in addition to the use of a bonded courier service with shipment tracking features, the information being shipped should have been sent in encrypted format. Given that unencrypted electronic records are analogous to paper records in that they may both be accessed in "plain text" or plain view, I believe that Commissioner Loukidelis' approach applies equally to the circumstances before me.

Additional guidance is provided by Investigation Report H2009-IR-004, a decision of the Office of the Information and Privacy Commissioner of Alberta Commissioner, Frank Work. This report involved a misdirected fax containing personal health information sent by a hospital records department, intended for a physician's office. While it did not involve a courier service, some of the findings made offer guidance here.

Section 60(1) of the Alberta *Health Information Act* requires that custodians take "reasonable steps" to protect against any reasonably anticipated unauthorized use, disclosure or unauthorized access to health information. Section 60(1) states:

> A custodian must take reasonable steps in accordance with the regulations to maintain administrative, technical and physical safeguards that will
>
> …
>
> (c) protect against any reasonably anticipated
>
> …
>
> (ii) unauthorized use, disclosure or modification of the health information or unauthorized access to the health information,

Report H2009-IR-004 found that the hospital did not take reasonable steps to protect health information against reasonably anticipated unauthorized disclosure by not assessing if the disclosure of health information via fax was reasonable in the circumstances, and by not evaluating whether there was a more secure method to transfer the information. While the circumstances of this case are different from those in H2009-IR-004, the impact of new technology solutions for transferring health information was addressed in the following comment:

> In conducting this investigation, I am mindful of the exponential uptake of information technology solutions in health care over the past five years. These innovations render the practice of manually faxing health information, at best, redundant and, at worst, an unnecessary risk to patient privacy.

The observations in Report H2009-IR-004 and the conclusion in Investigation Report F08-02 are instructive in examining the practices and procedures put in place by CCO to transfer the Screening Reports to PCPs via courier in paper format – the practice currently under review. As these decisions note, and as is expressly stated in the *Manual* referenced above, practices and procedures put in place with respect to the secure transfer of records of personal health information must be measured against *evolving standards and best practices*. Practices and procedures that may have been acceptable from a security and privacy perspective at one point in time may well become obsolete given the rapid development of technological safeguards.

In its submissions, CCO refers to two reports from my office involving privacy breaches that occurred when records of personal health information were transferred via courier. These reports are Report File No. HI-050004-1, dated June 30, 2005 and Report File No. HI-050010-1, dated August 10, 2005. CCO states:

> The IPC has issued reports concerning past occurrences in which paper documents containing [personal health information] were lost or stolen in the course of being delivered by a courier. However, these reports do not indicate that this delivery method is unacceptable.

It is important to note that both reports relate to actions taken in 2005 – an eternity ago, from a standards and technology perspective. As set out above, what may have been considered an acceptable practice or procedure in transferring records of personal health information at that time may not necessarily be considered a reasonable practice or procedure now. Also, in both

cases, the health information custodians involved in the breaches undertook to examine additional precautionary measures when transferring information, such as proactively de-identifying the personal health information contained in the records.

More important, it is dangerous to draw general conclusions based on a specific fact situation and apply those conclusions broadly to all instances where records of personal health information are being transferred. For example, most health information custodians will not have the size and sophistication of CCO, nor have the ready access to alternative methods of transferring records of personal health information. In other words, what constitutes reasonable practices and procedures to transfer records of personal health information for an agency like CCO may vary greatly from what may be reasonably expected from a single health care practitioner. As discussed in detail below, it is also important to draw a distinction between transferring multiple records of personal health information to PCPs, and transferring individual records to individual patients to whom the records of personal health information relate.

I recognize that there are privacy risks associated with all methods of transfer. The question at hand is whether CCO put into place practices and procedures to identify and minimize these risks, thereby protecting the privacy of individuals whose personal health information it received, and maintaining the confidentiality of that personal health information.

While CCO's practice and procedure of transferring Screening Reports in paper format using a courier service was the primary focus of this review, it also gave rise to one other issue, namely, whether CCO responded reasonably to the breach.

Consequently, the two issues that I will address below are:

(a) Did CCO meet its obligation to put into place practices and procedures to ensure the secure transfer of Screening Reports in paper format to PCPs using Canada Post's Xpresspost courier?

(b) Did CCO staff respond reasonably to the breach?

(a) Did CCO meet its obligation to put into place practices and procedures to ensure the secure transfer of Screening Reports in paper format to PCPs using Canada Post's Xpresspost courier?

This incident is an excellent illustration of the challenges of maintaining the confidentiality and privacy of thousands of Ontarians in a mass-scale distribution of paper records containing personal health information. In the context of the current review, I note that the loss of each courier package of Screening Reports effectively enabled full access to the sensitive information contained therein. To provide a sense of the magnitude of the risk, the original three packages of Screening Reports that were reported as undelivered at the end of April involved the personal health information of 2,388 individuals. At the conclusion of the site visits, it was determined that 17 packages of Screening Reports containing the personal health information of 7,130 individuals were lost and unaccounted for.

It comes as no surprise to security and privacy professionals that information will go missing from time to time. My office's experience has been, all too often, that such a loss is associated with sensitive personal information transferred in paper format, or in plain text via unencrypted means. We recognize that the pervasive risk of loss can never be fully eliminated. However, the impact of such losses can be dramatically minimized by taking steps that are reasonable in the circumstances to ensure that this information is protected from access by unauthorized persons and misuse, such as the implementation of encryption.

Although a breach of privacy relating to the personal health information of one individual is no less important than the loss of health information relating to thousands of individuals, it is important to consider the potential scope of a breach as part of the risk evaluation of any transfer process.

It is also important to consider the recipients and their access to technology. For example, it may not be appropriate to send records of personal health information to individual patients through electronic means as a number of those individuals may not have the necessary technology to access the information. However, the CCC is an ongoing, province-wide and long-term program involving the transfer of large volumes of records of personal health information, related to numerous individuals, to PCPs across the province. In such a case, the use of technology to ensure the secure transfer of records of personal health information is not only a feasible option, but a necessary one. Properly designed, these electronic systems can be made accessible, user friendly and highly secure.

This view is consistent with the Consultant's Report that reviewed the initial Pilot conducted by CCO. It identified two possible methods for securely transferring the Screening Reports to PCPs: the OntarioMD web portal, and by way of encrypted USB drives sent out via a bonded courier using a tracking service. Given the structure of the CCC program, either option could, and should, have been preferred over the one which was adopted.

The present breach was entirely preventable. It is unclear why the personal health information (which began in electronic form) could not have been encoded to physical CD or DVD media, or a USB drive, in encrypted and password protected formats. The password or key could then have been sent via separate channel, such as telephone or email (possibly even serving the additional functions of validating contact information, alerting recipients and/or confirming delivery/receipts). In this way, the privacy risks involving the loss or theft of Screening Reports could have been significantly mitigated. Further, most of the costs associated with mitigation and remediation (e.g., notifying thousands of patients and physicians), could have been obviated. To the best of our knowledge, this method of transfer was not contemplated by CCO.

I understand that, during the Pilot, some consideration was given to storing and transferring information on hardware-encrypted USB drives (a higher-quality and more secure type of USB drive that is capable of onboard cryptographic functions). This method of transfer was apparently rejected primarily due to a perception that the drives were not sufficiently secure or reliable. This was based on the fact that during the Pilot, the encrypted drives being trialed were recalled by the manufacturers due to a vulnerability discovered in the access control mechanism. Completely

rejecting any consideration of the hardware-encrypted USB drive on this basis is unreasonable. When deployed and used properly, hardware-encrypted USB drives are a proven method of storing and transferring sensitive information. The recall of one manufacturer's USB device does not mean that this method of transferring records of health information should have been rejected entirely – it is merely a reflection of a particular manufacturer's specific device.

As noted above, CCO also tested the OntarioMD web portal as a means of electronic transfer. This web portal enables physicians to directly access, download and even carry out limited actions on the records involved. Indeed, this initially appeared to be the preferred option of CCO over the use of paper records and was recommended in the Consultant's Report. In fact, as noted earlier, the 2010 PIA stated that, "the CCC Program should investigate the possibility of providing [Screening Reports] to physicians via portal for the next release scheduled for September 2011." However, it appears that due to a number of factors, the use of the OntarioMD web portal was deferred to a future point in time. CCO's representations submitted as part of this investigation did not indicate the intention of using the portal for its next scheduled release, which I note, was initially intended to occur post-September 2011. In my view, the OntarioMD web portal should have remained the preferred option. The problems identified with that option during the Pilot should have been reviewed and addressed by CCO, in the interim period between the Pilot and the first mass distribution to PCPs that occurred in February.

The Consultant's Report indicated that the timely delivery of follow-up Screening Reports was essential to the effectiveness of the CCC. As noted in the 2010 PIA, there were time constraints that led to the conclusion that the web portal solution was not feasible for the transfer that was planned for February and March of 2011. The transfer of paper records was evidently intended as a provisional method of delivery until such time as the web portal or similar method of electronic transfer became feasible. This being the case, it remains unclear why more secure methods of transfer, such as the encrypted devices described above, were not fully considered by CCO.

In summary, I find that CCO, by transferring the Screening Reports to PCPs in paper format, failed to put in place reasonable practices and procedures for the purpose of protecting the privacy of the individuals whose personal health information was contained in the reports, and for the purpose of maintaining the confidentiality of that information, despite having been alerted to the potential risk of doing so.

Surprisingly, in its submissions, CCO expressly stated:

> …CCO believes that mailing [personal health information] in paper format through a secure courier service is an acceptable practice, provided that security safeguards (e.g. courier services that track packages and require signatures required upon delivery) are followed to ensure safe delivery of [personal health information.]

Given that these were the exact circumstances that led to the breach being investigated, I am astounded that CCO continues to take the position that couriering Screening Reports in paper format remains an acceptable practice. It is clear that the risks to privacy of adopting this approach were brought to their attention by their Consultant when evaluating the Pilot.

Indeed, the events set out in this Order justified the Consultant's fears. CCO had two alternative methods of transfer available to it, both of which had been identified by the Consultant as more privacy-protective. It appears that these alternatives were rejected by CCO on the basis that they might require some additional work to implement and to accommodate the convenience of the recipient physicians. These are not acceptable grounds for implementing a method of transfer for which far greater privacy risks had been identified. As a result, I will be ordering CCO to discontinue the practice of transferring Screening Reports to PCPs in paper format.

After receipt of its submissions, on September 29, 2011, CCO wrote to my office and stated that it had conducted a review of options to determine the appropriate vehicle for the next transfer of the Screening Reports scheduled for the spring of 2012. It also stated that a number of options were considered, including encrypted CD, facsimile, courier with signature, the OntarioMD web portal and the development of a CCO physician web portal. Following its review, CCO is proposing to develop a CCO web portal, and the associated user registration and identity management systems for the distribution of the Screening Reports. CCO has not provided my office with the details of this review nor any rationale for this decision.

The decision to use a web portal is certainly advisable. However, the creation of an entirely new portal may not be the preferred option.

The creation and use of a centralized web portal for making records of personal health information directly available to physicians in electronic format holds considerable potential for assuring greater security of data in transit, through the use of strong authentication and cryptography (as well as for logging and validating receipt). I recognize that such web portals also introduce certain threats and risks that are qualitatively and quantitatively different from those associated with couriering paper records, due to the potential for online loss or theft, through unauthorized access. However, strong privacy and security measures for the protection of data may be proactively and directly built into the systems involved. Once in place, these measures would then be subjected to the appropriate reviews and scrutiny necessary to ensure effectiveness and audit functionality prior to adoption.

While I am pleased that CCO is proposing a significantly more secure method of transferring Screening Reports to PCPs, I require far greater detail regarding its proposed option, and in particular, the reasons why it has decided to reject the OntarioMD web portal. It is not at all clear why the OntarioMD web portal option was rejected – on the face of it, I do not accept that the proposal to establish its own portal is the best option. Given that the OntarioMD web portal has been established by the Ministry, for purposes such as those at issue in this review, this option requires serious consideration by CCO. In addition, OntarioMD is the solution being advanced by the government of Ontario for secure exchanges of communications and health information among health care practitioners in this province. This would appear to be the web portal of choice, absent serious problems with it that have yet to be identified.

Accordingly, I will be ordering CCO to provide a full report to my office on the advantages and disadvantages of transferring the Screening Reports in electronic format via the OntarioMD web portal, as compared to the proposed CCO web portal. This report is to include a complete

assessment of the security and privacy protective measures that will be built into the architecture of the proposed CCO web portal. It should also contain a comparison of those measures against the existing and potentially enhanced security and privacy measures of the OntarioMD web portal.

To be clear, CCO must obtain the approval of my office for the selected method prior to resuming the transfer of Screening Reports to Primary Care Physicians.

(b) Did CCO staff respond reasonably to the breach?

The circumstances of this review have uncovered another gap in the practices of CCO. While staff in the CCC Call Centre were alerted to the fact that three Screening Reports had not been received on April 26, 2011, no one notified the CCC Program Manager or CCO Privacy Office until June 1, 2011. CCO stated the incident was not reported because "it was not apparent [to CCC Call Centre staff] that there had been a breach or that there was a risk of a breach prior to June 1, 2011." CCO stated that the Call Centre staff determined that a breach may have occurred after being informed that the matter was being escalated within Canada Post on June 1, 2011.

It is surprising that CCO would take such a position in this review. CCC Call Centre staff were aware that the Screening Reports contained the sensitive personal health information of a large number of individuals. When three of the packages were reported missing, this matter should have been reported immediately to the Privacy Specialist or the CCO Chief Privacy Officer. There was no apparent reason to wait before advising them of this potential breach – it is not up to the Call Centre to make determinations relating to potential data breaches. The Privacy Specialist or the CCO Chief Privacy Officer should have been alerted immediately.

CCO had been made aware of the risk that the paper Screening Reports could be lost in transit. Indeed, the 2010 PIA and the Consultant's Report had both alerted CCO to this risk. Furthermore, Recommendation 6 of the Privacy Risk Register relating to the 2010 PIA, states:

> ***The CCC Program should ensure that privacy escalation process is in place for any potential breach calls received from physicians and patients.*** [Emphasis added.]

As stated above, staff at CCC's Call Centre were alerted on April 26, 2011 that three physicians had not received their Screening Reports. This was a full month after they had been sent via courier. Although the Privacy Risk Register specifically contemplated that this might happen, there is no indication that the privacy escalation process was put in place. While there was some delay in attempting to locate these reports, it should have been apparent that there was a risk that these Screening Reports were lost. Instead, the matter was only brought to the attention of those outside of the CCC Call Centre and LMG during a working group meeting on May 30, 2011 – over a month after having been alerted of the problem, at which point a decision was made to notify the appropriate CCC Program Manager.

I am equally concerned that despite the fact that it was known that three packages were missing, another month and a half passed before CCO took any action to determine the scope of the breach. I note that based on the CCO and LMG's submissions, neither availed themselves of the individual package tracking function until June 17, 2011 and, by this time, it was too late to use the tracking function for many of the packages.

In its submissions to my office, CCO provided a copy of the CCC *Privacy Breach Management Procedure*. The procedure, dated April 1, 2008, and revised on October 27, 2009, outlines how CCC will identify and handle privacy breaches. It also defines a privacy breach as follows:

> A privacy breach, whether intentional or inadvertent, is the misuse or improper/unauthorized collection, use, or disclosure of personal health information.

Once a privacy breach has been identified, the CCC *Privacy Breach Management Procedure* requires CCC staff to report the matter to the CCC Privacy Specialist or to the CCO Chief Privacy Officer. The following excerpt from the *Privacy Breach Management Procedure* outlines the obligations and process with regards to reporting, stating, in part:

7. All CCC staff are responsible for *immediately reporting privacy breaches, suspected privacy breaches, and/or privacy risks they believe may lead to a privacy breach in the future.*
8. Privacy breaches and/or risks must be immediately reported to the CCC Privacy Specialist in person, via email (privacy@cancercare.on.ca), or phone at 416-971-9800 ext. 3631. CCC staff may also report privacy breaches and/or privacy risks to the CPO when they are uncomfortable reporting them to the CCC Privacy Specialist. The Privacy Director will immediately investigate the privacy breach or privacy risk in accordance with the CCO Privacy Breach Policy.
9. The CCC Privacy Specialist is obligated to report privacy breaches and/or privacy risks in which he or she may be involved to the Privacy Director.
10. CCC extends "whistleblower" protection to CCC staff who report a breach or potential contravention of Ontario's Personal Health Information Protection Act, 2004 (PHIPA) or who refuse to perform a transaction that they believe to be in contravention of PHIPA or the CCC Privacy Policy.
11. The CCC Privacy Specialist will notify the Privacy Director of the privacy breach. Notification will include the description of the breach.
12. The Privacy Director will notify senior management and others, including the Office of the Information and Privacy Commissioner/Ontario (IPC), where appropriate. [Emphasis added.]

While CCO submitted that the CCC Call Centre staff acted according to their procedure, it acknowledged at page 11 of the *CCO Privacy Breach Report – SAR* that, "it may be useful to strengthen the language in the policy and training to give clearer examples of 'privacy risks' that may lead to a breach."

In my view, the circumstances of these lost or unaccounted Screening Reports constitute an inadvertent disclosure of personal health information and, therefore, fall within the definition of a privacy breach set out in the *Privacy Breach Management Procedure*. By failing to identify the fact that a privacy breach or potential privacy breach had occurred, and by failing to *immediately* report the breach or potential breach to the Privacy Specialist or CCO Chief Privacy Officer, CCC Call Centre staff did not comply with its own policies.

A key component to breach management is immediately identifying such an event, in an effort to contain the harm. The delays in the reporting of the breach to the Privacy Specialist or the CCO Chief Privacy Officer resulted in a delay in the containment efforts. It is essential that individuals within an organization understand what constitutes a "privacy breach", "suspected privacy breach" and "privacy risk" and the indicators of such events. I will include an order provision below requiring CCO to amend its *Privacy Breach Management Procedure* to ensure compliance with section 13(2).

A review of this incident also indicates the need for further staff training regarding breach management. The circumstances of this breach indicate that CCC staff could not identify the risk factors associated with a potential breach. Consequently, in the order provisions that follow I will also order that CCO arrange for additional training of CCC Call Centre staff regarding the breach management process.

For all of these reasons, I find that CCO failed to put in place reasonable practices and procedures for the purpose of protecting the privacy of the individuals whose personal health information was contained in the Screening Reports and for maintaining the confidentiality of that information.

7.0 ORDER

I order Cancer Care Ontario to put into place practices and procedures to protect the privacy of individuals whose personal health information it receives as part of the ColonCancerCheck program and for maintaining the confidentiality of the information as required by section 13(2) of the Regulation. Specifically, I order Cancer Care Ontario to:

1. Discontinue the practice of transferring Screening Reports containing personal health information to Primary Care Physicians in paper format;

2. Provide a full report to my office on the advantages and disadvantages of transferring the Screening Reports in electronic format via the OntarioMD web portal, as compared to the proposed CCO web portal. This report is to include a complete assessment of the security and privacy protective measures that will be built into the architecture of the proposed CCO web portal. It should also contain a comparison of those measures against the existing and potentially enhanced security and privacy measures of the OntarioMD web portal. CCO must obtain the approval of my office prior to resuming the transfer of Screening Reports to Primary Care Physicians.

3. Review the *CCC Privacy Breach Management Procedure* and any related policies and procedures to clarify and ensure that those having an employment, contractual or other relationship with Cancer Care Ontario are fully aware of their responsibility to immediately report any privacy breaches, suspected privacy breaches and/or privacy risks to appropriate individuals at Cancer Care Ontario with responsibility for privacy issues.

4. Conduct additional training with those having an employment, contractual or other relationship with Cancer Care Ontario to ensure that they are fully aware of their duties and responsibilities under the *CCC Privacy Breach Management Procedure*.

In order to verify compliance with Order Provisions 3 and 4, I require that Cancer Care Ontario provide me with proof of compliance no later than January 13, 2012.

I remain seized of this matter to deal with any issues that may be outstanding as a result of Cancer Care Ontario's review, and as a result of the report to be provided to my office by Cancer Care Ontario, or any other issues that may arise, including the right to make any further Order provisions that may be necessary.

October 13, 2011

Ann Cavoukian, Ph.D.
Commissioner

Date

Information & 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
Web site: www.ipc.on.ca
Email: info@ipc.on.ca