Ann Cavoukian, Ph.D.
Information & Privacy Commissioner
Ontario, Canada

Fact Sheet

Number 18
August 2012

The Secure Transfer of Personal Health Information

To ensure the timely and effective delivery of healthcare, health information custodians (custodians) may need to transfer personal health information. The need for vigilance in safeguarding the privacy of individuals during such transfers was highlighted when several courier packages sent by Cancer Care Ontario, containing the colon cancer screening information of more than 7,000 individuals, were lost. Following the loss, the Information and Privacy Commissioner of Ontario (IPC) ordered Cancer Care Ontario to stop transferring these records in paper format and to explore secure electronic means of transfer.[1] This Fact Sheet explains what this Order means for custodians.

Although the Order is directed at Cancer Care Ontario and was based on the particular circumstances at issue, it provides guidance that may help custodians minimize the risk of breaches when transferring records of personal health information. The Fact Sheet outlines a number of factors that should be considered by custodians in developing policies, procedures and practices for securely transferring records in paper and electronic format, recognizing that while some custodians have embraced electronic records, for others it is a work-in-progress.

1 Order HO-011

Order HO-011

Cancer Care Ontario used a courier service to transfer records containing colon cancer screening information to physicians in paper format after considering but rejecting other options, including transfers via a web portal or encrypted USB drives. It was later discovered that the colon cancer screening information of over 7,000 individuals had not been received by the physicians.

In reviewing this incident, the IPC considered the following factors:

- the characteristics of the person or organization transferring the records;
- the characteristics of the person or organization receiving the records;
- the number of individuals whose personal health information was contained in the records;
- the volume and frequency of the transfer(s); and

- the availability of alternative methods of transfer, and the risks associated with each.

Applying these factors, the IPC concluded that reasonable steps were not taken to ensure that the records were transferred in a secure manner for the following reasons:

- Cancer Care Ontario is a large, sophisticated organization with the resources to adopt a more secure method of transfer than the paper-based method employed;
- the persons who received the records were physicians, who could reasonably be expected to have the technology necessary to access personal health information electronically;
- the records contained the personal health information of large numbers of individuals and formed part of an ongoing, province-wide program, therefore, the scope and risk associated with any potential breach was substantial;[2] and
- other more secure methods of transfer were available, including electronic options.

What does the Order mean for health information custodians?

While Cancer Care Ontario was ordered to stop transferring records containing colon cancer screening information in paper format, this does not mean that records of personal health information may never be transferred in paper format, including by bonded courier or regular mail. The reasonableness of employing a particular method of secure transfer will depend on the circumstances. The Order listed a number of factors, described below, that custodians should consider when choosing a secure method of transfer. These factors are not mutually exclusive and must be considered together in assessing whether a particular method of secure transfer is reasonable in the circumstances.

Characteristics of the person or organization transferring the records

What is expected of an agency like Cancer Care Ontario may vary greatly from what is expected of a sole practitioner. The size, sophistication and resources of the custodian should be considered in determining what methods of secure transfer are reasonably available.

Characteristics of the person or organization receiving the records

The custodian transferring the records should also consider whether the recipient has the capacity to access the records through the method of transfer being contemplated. For example, it may not be reasonable to expect individual patients to have the technology necessary to access records electronically. However, the Order notes that where it is reasonable to expect the recipient to have the necessary capacity, the personal preference of the recipient is not a valid reason for choosing a method that poses greater risks to privacy.

2 At the outset, the personal health information of over 20,000 individuals was unaccounted for. However, after the IPC requested site visits to be conducted, the number was reduced to approximately 7,000 individuals.

The number of individuals whose information is contained in the records

The number of individuals whose personal health information is contained in the records being transferred will determine the scope of any potential privacy breach – this is an important consideration in selecting a method of secure transfer.

Volume and frequency of transfer

As the volume and frequency of transfers increase, so too does the risk. Transfers involving the widespread distribution of large numbers of records of personal health information, or that recur on a regular basis, or form part of an ongoing or long-term program, pose increased risks to privacy.

Availability of alternative methods of transfer and their associated risks

In selecting a method of secure transfer, it is important to identify and consider all available alternatives that do not interfere with the timely and effective delivery of health care. New methods may become available as technology evolves and privacy-enhancing solutions emerge. Custodians should, whenever possible, make efforts to learn about changing industry standards and best practices, including through guidance provided by the IPC in its orders, guidelines and fact sheets.

Once all the alternative methods of transfer have been identified, custodians should assess the risks to privacy and confidentiality posed by each method. This will enable custodians to identify measures that can mitigate the risks associated with each method, and select a reasonable method that carries a level of risk that is proportional to the degree of harm that could result from any breach. Assessing such risks will not necessarily require a formal privacy impact assessment.

Formal privacy impact assessments are recommended as a best practice where the personal health information of a large number of individuals is contained in the records, where there is a significant volume of records being transferred and/or where the transfer forms part of an ongoing program. Custodians who do not have the knowledge or expertise necessary to conduct a formal privacy impact assessment should consider consulting with appropriate experts.

Put it in writing: Policies, procedures and practices

Custodians will want to consider all of the factors cited above as they develop and implement written policies and procedures for the secure transfer of records in paper and electronic format. It is recommended that one's policies and procedures set out the approved methods of secure transfer and prohibit the use of any other method. The approved methods should be reviewed regularly to ensure that they are consistent with evolving privacy and security standards and best practices. Practices and procedures that are considered acceptable at one point in time may become obsolete as technology and security standards change.

As a best practice, the policies and procedures should set out:

- circumstances in which records of personal health information may be transferred through each of the approved methods;
- procedures to be followed in transferring records through each of the approved methods;
- administrative, technical and physical safeguards that must be implemented in transferring records through each of the approved methods;
- the content of any documentation to be completed, including the date, time and method of transfer; the name of the person or organization receiving the records; and the nature of the records transferred; and
- procedures for confirming receipt of the transfer.

Despite the best-laid plans, a privacy breach may occur … how do you prepare for this?

Custodians should develop and implement written policies and procedures to identify, report, contain, investigate and remediate privacy breaches or suspected breaches, as well as notify affected individuals of such breaches.

The policies and procedures should define what constitutes a privacy breach or suspected privacy breach, including those that occur during transfer. A suspected privacy breach should be defined to include circumstances where the records have not been received within a reasonable amount of time following the transfer.

The policies and procedures should also require employees, contractors and others acting on behalf of the custodian to notify the custodian of a privacy breach or suspected privacy breach at the first reasonable opportunity[3] and should require the custodian to notify affected individuals of a privacy breach.[4]

For further information, please refer to *What to do When Faced With a Privacy Breach: Guidelines for the Health Sector*, published by the IPC.

Training and Education

Custodians should provide education and training on their policies and procedures for secure transfer and for managing privacy breaches. [5]

Requirements of the *Act*

The *Personal Health Information Protection Act* establishes rules to ensure that custodians protect privacy and maintain confidentiality, while at the same time allowing for the timely and effective delivery of health care. Custodians must transfer records of personal health information in a secure manner[6] and take steps that are reasonable in the circumstances to ensure the security of such

3 Section 17(3) of the *Act*
4 Section 12(2) of the *Act*
5 Section 15 of the *Act*
6 Section 13(1) of the *Act*

information.[7] Custodians must also ensure that personal health information is not transferred if other information (such as de-identified or aggregate information) would be sufficient. Where personal health information is needed, only the minimal amount necessary may be transferred.[8]

7 Section 12(1) of the *Act*
8 Section 30 of the *Act*

Additional IPC Guidance

Guidelines on Facsimile Transmission Security (January 2003)

Order HO-011 (October 2011)

Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act (October 2005)

Privacy Protection Principles for Electronic Mail Systems (February 1994)

What to do When Faced with a Privacy Breach: Guidelines for the Health Sector (March 2012)