# Detecting and Deterring Unauthorized Access to Personal Health Information

Information and Privacy Commissioner of Ontario

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

# TABLE OF CONTENTS

# INTRODUCTION

The relationship between individuals and their health care providers is based on trust. Individuals provide intimate details about their health and wellness, in confidence, to their health care providers in order to receive the best care and treatment. Personal health information is shared with health care providers with the expectation that it will be used and disclosed, to the extent reasonably necessary, for the purposes of providing or facilitating the provision of health care or for related purposes. Individuals do not expect their personal health information to be collected, used or disclosed by persons who are not involved in their health care, without their express consent, for purposes that are not related to the provision of health care and not authorized by law. If individuals' expectations of privacy and confidentiality are not fulfilled, the relationships between individuals and their health care providers may be irreparably damaged. This may have serious repercussions for individuals, health care providers and the entire health sector.

In Ontario, the *Personal Health Information Protection Act (PHIPA)* sets out rules for the collection, use and disclosure of personal health information by health information custodians (custodians) and their agents. Custodians are persons and organizations, such as health care practitioners and hospitals, that have custody or control of personal health information for purposes related to the delivery of health care. Agents are persons, such as employees, independent contractors, physicians with privileges and volunteers, who act on behalf of custodians in respect of personal health information.

*PHIPA* permits custodians to collect, use and disclose personal health information for the purposes of providing or assisting in the provision of health care based on implied or assumed implied consent but prohibit the collection, use and disclosure of personal health information for any other purpose without the express consent of the individual, unless permitted or required by *PHIPA*. *PHIPA* requires custodians to take steps that are reasonable in the circumstances to ensure that personal health information in their custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing personal health information are protected against unauthorized copying, modification or disposal.

Recently, there have been a number of cases in which custodians or their agents have used or disclosed personal health information, without the consent of individuals, for purposes that are not permitted or required by *PHIPA*. While many of these cases involved access to the electronic records of personal health information of family members, friends, co-workers, and neighbours, as well as celebrities, politicians and other well-known individuals, other cases involved access to the electronic records of individuals who did not have any relationship with the custodian or agent. The use or disclosure of personal health information for such purposes is commonly referred to as "unauthorized access." Unauthorized access, including the viewing of personal health information in electronic information systems, may be motivated by a number of factors including interpersonal conflicts, curiosity, personal gain or concern about the health and well-being of individuals.

Unauthorized access appears to be a growing problem in the health sector in Ontario. The purpose of this paper is to shed light on the extent of the problem and the potential consequences for individuals, custodians and their agents, and the entire health sector, and to provide guidance to custodians on minimizing the risk of unauthorized access by their agents.

# THE BENEFITS AND RISKS OF ELECTRONIC RECORDS

Increasingly, the health sector has been transitioning from paper-based records to electronic records. For example, a 2013 National Physician Survey found that 64% of family physicians/general practitioners in Canada use electronic records to enter and retrieve clinical notes.[1] According to Canada Health Infoway, there are more than 62,000 users of electronic records of personal health information across Canada, an increase of more than 700% since 2006.[2]

The benefits of electronic records are numerous. An electronic record can be retrieved quickly and easily by those who are involved in providing health care to an individual, regardless of where they are located. Electronic records require less space and fewer administrative resources to maintain and are generally easier to read and locate than paper-based records which may be handwritten, sometimes in an illegible manner, incomplete and dispersed across various locations. Electronic records may support improved clinical decision-making leading to more effective diagnosis and treatment; greater safety through better availability of comprehensive, up-to-date and accurate personal health information; increased efficiency; and improved access to services. Electronic records can also be designed to enhance the privacy of individuals and the security of personal health information through safeguards such as access controls, logging and auditing functionality, and encryption.

While electronic records have many potential benefits such as enhanced accessibility, transferability and portability, these features also pose unique privacy risks. Electronic records have the potential to allow for the collection, use and disclosure of large amounts of personal health information from diverse sources at the press of a key and are more likely to attract hackers and others with malicious intent. Electronic records may also increase the risk of unauthorized access to personal health information by custodians and their agents with role-based access privileges. A report analyzing more than 63,000 security breaches from 95 countries found that "insider and privilege misuse," defined as any internal unapproved or malicious use of organizational resources,

1 The College of Family Physicians of Canada, Canadian Medical Association, The Royal College of Physicians and Surgeons of Canada, *National Physician Survey 2013*. Available online at: http://nationalphysiciansurvey.ca/surveys/2013-survey/survey-results/

2 Canada Health Infoway, *Annual Report 2013-2014*. Available online at: https://www.infoway-inforoute.ca/index.php/resources/infoway-corporate/annual-reports

accounted for 15% of breaches suffered by health care organizations and 85% of those breaches involved electronic rather than paper-based records.[3]

Personal health information in electronic records can be more easily and quickly collected, used and disclosed for unauthorized purposes, potentially increasing the magnitude and severity of a privacy breach.

Unauthorized access to personal information is a concern across all industry sectors. In a Ponemon Institute study of privileged users, such as database administrators, network engineers and IT security practitioners across a variety of industry sectors in the United States, 65% of respondents stated that it is very likely or likely that privileged users access sensitive or confidential information out of curiosity.[4] In another Ponemon Institute study of IT practitioners across industry sectors in the United States, 78% of respondents indicated that negligent or malicious employees or other insiders have been responsible for at least one privacy breach within their organizations over the past two years.[5]

Unauthorized access to personal health information in electronic information systems is also a major issue for the health sector specifically. There are no Ontario-specific statistics as to the frequency of unauthorized access to personal health information by custodians and their agents. However, the number of cases reported in Ontario and other jurisdictions in Canada, as well as reports from the United States, appear to suggest that this issue is a pervasive problem for the health sector throughout Canada and the United States. For example, one report from the United States found that 52% of health care organizations believe they are vulnerable or extremely vulnerable to insider threats and 61% of health care security professionals say that non-technical employees with legitimate access to personal health information and information technology assets pose the biggest threat of an insider attack.[6]

3 Verizon, *2014 Data Breach Investigations Report*. Available online at: http://www.verizonenterprise.com/DBIR/2014/ and http://www.verizonenterprise.com/resources/factsheets/fs_2014-dbir-industries-healthcare-services-threat-landscape_en_xg.pdf

4 Ponemon Institute LLC, *Privileged User Abuse & The Insider Threat*, May 2014. Available online at: http://www.trustedcs.com/resources/whitepapers/Ponemon-RaytheonPrivilegedUserAbuseResearchReport.pdf

5 Ponemon Institute LLC, *The Human Factor in Data Protection*, January 2012. Available online at: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_trend-micro_ponemon-survey-2012.pdf

6 Jon Oltsik, *Vormetric/ESG Insider Threat Report: Profile on Health Care*, January 2104. Available online at: http://enterprise-encryption.vormetric.com/2014-Vormetric-Insider-Threat-Report-Healthcare.html (log in required)

# THE IMPACT OF UNAUTHORIZED ACCESS

## HARM TO INDIVIDUALS

Unauthorized access to personal health information can have significant consequences for all involved. Individuals whose personal health information is the subject of unauthorized access may suffer discrimination, stigmatization and emotional or psychological harm. The harm may be compounded when the unauthorized access comes at a time when the individual is experiencing a serious or life-threating illness and is most vulnerable to the adverse effects of stress. Individuals may be deterred from seeking future testing or treatment and may withhold or falsify personal health information provided to custodians and their agents out of fear of unauthorized access. Individuals may also lose trust or confidence in the health system. A survey sponsored by Canada Health Infoway found that 85% of Canadians believe that individuals withhold personal health information from their doctors, with 33% believing this is due to concerns about other staff viewing their personal health information.[7]

## REPUTATIONAL DAMAGE

Unauthorized access to personal health information may cause irreparable damage to the reputation of custodians and their agents, as well as to the relationships they have with individuals who have entrusted them with their personal health information. To the extent that individuals lose trust and confidence in custodians' and their agents' ability to protect their personal health information, they may withhold vital information and/or impose conditions or restrictions on the collection, use and disclosure of their personal health information.

The efficient and effective delivery of health care depends on the availability of accurate, complete and up-to-date personal health information. If individuals do not provide such information due to a lack of trust and concerns about privacy, this may impact the quality of health care provided, as well as patient safety. It may also affect the quality of health information that is available for secondary purposes such as health research and health system planning. Further, if individuals impose conditions or restrictions on the collection, use and disclosure of their personal health information rather than simply allowing custodians to rely on implied consent, this may not only impede or delay the delivery of health care, but may also increase administrative costs for custodians and the entire health system.

7 Ipsos Reid, *What Canadians Think Electronic Health Information and Privacy Survey 2012*. Available online at: https://www.infoway-inforoute.ca/index.php/resources/reports/privacy

## DISCIPLINARY ACTION

Unauthorized access to personal health information by agents may result in disciplinary action such as termination or suspension of their employment, contractual or other relationship with the custodian. Regulated health professionals may also be reported to their regulatory college, potentially resulting in an investigation, a finding of professional misconduct and further discipline. This could have serious implications for future employment and professional opportunities.

For example, a registered nurse who viewed the electronic record of personal health information of the estranged spouse of her boyfriend was disciplined by the College of Nurses of Ontario. Her certificate of registration was suspended for six weeks; terms, conditions and limitations were imposed on her certificate of registration; and she was reprimanded by the panel. One of the conditions imposed on her was that, for a year after returning to practice, she must provide her employers with a copy of the order and notice of hearing or, if available, the written decision and reasons.[8]

In Alberta, a pharmacist who viewed the records of a number of women from her church and posted prescription information on Facebook, in contravention of Alberta's *Health Information Act*, was disciplined by the College of Pharmacists. The pharmacist's practice permit was suspended for four months and she was verbally reprimanded and required to pay a $4,000 fine, in addition to hearing costs. Furthermore, a copy of the decision, including the name of the pharmacist, was sent to all pharmacy regulatory bodies in Canada.[9]

In another case in Alberta, a physician who used the provincial electronic health record, Alberta Netcare, to access personal health information during the course of a divorce proceeding was disciplined by the College of Physicians and Surgeons of Alberta. Her practice permit was suspended for 60 days and she was ordered to complete an ethics course and to pay the costs of the hearing and investigation.[10]

8 Discipline Committee of the College of Nurses of Ontario, *Between: College of Nurses of Ontario and Registration No.HB00883*, heard July 2008. Available online at: http://www.cno.org/Global/2-HowWeProtectThePublic/ih/decisions/fulltext/pdf/2009/Kerry%20Smith,%20HB00883,%20July%2010,%202008.pdf

9 Available online at: https://pharmacists.ab.ca/sites/default/files/SonggadanDecision.pdf

10 College of Physicians and Surgeons of Alberta, *In the Matter of a Hearing Under the Health Professions Act*, *R.S.A. 2000,c.C-7*. Available online at: http://cpsa.ab.ca/Libraries/pro_complaints_disc/011469-000015972511-4.pdf

## PRIVACY INVESTIGATIONS

Unauthorized access to personal health information may result in an investigation and an order by the Information and Privacy Commissioner of Ontario. To date, the Information and Privacy Commissioner of Ontario has issued three orders regarding unauthorized access to personal health information by custodians and their agents.

In 2006, an order was issued in the case of a registered nurse who, on ten occasions, viewed the electronic record of the estranged spouse of her boyfriend, to whom she was not providing care. The order found that the nurse used and disclosed personal health information in contravention of *PHIPA* and that the hospital did not take steps that were reasonable in the circumstances to safeguard the information. Hospital staff failed to follow internal privacy policies, and the hospital failed to take immediate action to prevent any further unauthorized use or disclosure of personal health information.[11]

In another case involving the same hospital, a diagnostic imaging technologist viewed, on six separate occasions, the electronic record of personal health information of the current spouse of her former spouse, to whom she was not providing care. The order found that the technologist used personal health information in contravention of *PHIPA* and that the hospital failed to comply with its information practices and did not take steps that were reasonable in the circumstances to safeguard personal health information.[12]

More recently, in 2014, an order was issued in the case of two hospital employees in clerical positions who used and/or disclosed the personal health information of mothers who had recently given birth for the purpose of selling or marketing Registered Educational Savings Plans (RESPs). The order found that personal health information was used and/or disclosed in contravention of *PHIPA* and that the hospital did not take steps that were reasonable in the circumstances to safeguard personal health information, did not have information practices that comply with *PHIPA*, and failed to comply with its information practices.[13] In all three cases of unauthorized access, the hospitals were ordered to take a number of remedial actions in order to prevent or reduce the risk of similar privacy breaches in the future.

Other privacy oversight bodies across Canada have also issued numerous reports regarding unauthorized access to personal health information. For

11 Information and Privacy Commissioner of Ontario, *Order HO-002*, issued July 2006. Available online at: http://www.ipc.on.ca/images/Findings/up-HO_002.pdf

12 Information and Privacy Commissioner of Ontario, *Order HO-010*, issued December 2010. Available online at: http://www.ipc.on.ca/images/Findings/ho-010.pdf

13 Information and Privacy Commissioner of Ontario, *Order HO-013*, issued December 2014. Available online at:http://www.ipc.on.ca/images/Findings/ho-013.pdf

example, the Information and Privacy Commissioner of Alberta issued an investigation report regarding the physician who used Alberta Netcare to view the personal health information of a partner's former spouse, and mother and girlfriend of the former spouse, to whom the physician was not providing care, during the course of a divorce proceeding. The physician accessed personal health information 21 times over a period of 15 months using the accounts of 12 different colleagues who failed to log out of Alberta Netcare.[14] The Information and Privacy Commissioner of Saskatchewan issued an investigation report regarding a pharmacist who viewed the drug profiles of three individuals to whom he was no longer providing care out of concern for their well-being.[15] Also in Saskatchewan, an investigation report was issued in relation to three separate cases where employees of the Regina Qu'Appelle Regional Health Authority viewed and/or modified personal health information in electronic information systems in contravention of the *Health Information Protection Act*.[16] In Manitoba, the Ombudsman issued a report regarding an employee of CancerCare Manitoba who viewed a newly created electronic record containing the name and cancer registry number of a child whose family had a strained relationship with the employee. The employee was not providing care to the child when the personal health information was viewed.[17]

## PROSECUTIONS AND FINES FOR OFFENCES

Unauthorized access to personal health information can also result in a prosecution. In Ontario, a person is guilty of an offence if the person wilfully collects, uses or discloses personal health information in contravention of *PHIPA* or its regulations. If convicted of an offence, a person is liable to a fine of up to $50,000, while an organization is liable to a fine of up to $250,000.

To date, only one prosecution for an offence has been commenced under *PHIPA*. In 2011, North Bay Regional Health Center concluded that a nurse accessed the personal health information of 5,800 patients in contravention of *PHIPA*. The nurse was charged for wilfully collecting, using or disclosing personal health information in contravention of PHIPA or its regulations.[18]

14 Information and Privacy Commissioner of Alberta, *Report of an investigation concerning misuse of the Alberta Electronic Health Record (Netcare) Covenant Health Investigation Report H2011-IR-004*, issued November 2011. Available online at: http://www.oipc.ab.ca/downloads/documentloader.ashx?id=2912

15 Saskatchewan Office of the Information and Privacy Commissioner, Investigation Report H-2010-001 L & M Pharmacy Inc. *Sunrise Regional Health Authority Ministry of Health*, issued March 2010. Available online at: http://www.oipc.sk.ca/Reports/H-2010-001,%20March%2023%202010.pdf

16 Saskatchewan Office of the Information and Privacy Commissioner, *Investigation Report H-2013-001 Regina Qu'Appelle Regional Health Authority*, issued February 2013. Available online at: http://www.oipc.sk.ca/What's%20New/IR-H-2013-001/Investigation%20Report%20H-2013-001.pdf

17 Manitoba Ombudsman, *Report with Recommendations Issued on July 20, 2012 and Response to the Recommendations under The Personal Health Information Act Cases 2011-0513 and 2011-0514* CancerCare Manitoba. Available online at: https://www.ombudsman.mb.ca/uploads/document/files/cases2011-0513-0514-en.pdf

18 Maria Calabrese, North Bay Nugget, *Hospital Ordered to Disclose Records*, July 2013. Available online at: http://www.nugget.ca/2013/07/05/hospital-ordered-to-disclose-record

The fact that charges may be laid will be an effective deterrent only to the extent that custodians and their agents believe that such measures are going to be used in appropriate circumstances. Given the current pervasiveness of the problem of unauthorized access, it may be necessary to increase the number of prosecutions to warn custodians and their agents that unauthorized access is not acceptable and will not be tolerated.

There have been a number of prosecutions for unauthorized access in other provinces. For example, in Alberta, a medical office clerk was charged under the *Health Information Act* for accessing the personal health information of the wife of a man with whom she was having an affair. She pled guilty and was fined $10,000.[19] The pharmacist in Alberta who viewed the records of women from her church and posted prescription information on Facebook was also charged under the Health Information Act and was required to pay a fine and hearing costs totalling $15,000.[20] As well, in Alberta, a woman was convicted of knowingly accessing the personal health information of 34 people in contravention of the *Health Information Act*, along with three *Criminal Code* offences related to falsified documents. She received a four month conditional sentence, followed by eight months of probation, in relation to the criminal offences and a $500 fine in relation to the *Health Information Act* offence.[21] In 2014, in Newfoundland and Labrador, a former Western Health employee pleaded guilty to collecting, using or disclosing personal health information contrary to the *Personal Health Information Act* and was fined $5,000.[22] Also in 2014, a former Eastern Health employee in Newfoundland and Labrador was fined $1,000 for collecting, using or disclosing personal health information contrary to the *Personal Health Information Act*.[23]

## LEGAL ACTIONS

In Ontario, a person affected by an order of the Information and Privacy Commissioner or a person affected by conduct leading to a conviction for an offence under *PHIPA*, that has become final, may begin proceedings for damages for actual harm suffered. *PHIPA* further states that where the harm results from wilful or reckless conduct, the court may award an amount not exceeding $10,000 for mental anguish.

19 Michael Whitt and LeRoy Brower, *Health Service Provider Fined $10,000*, Healthcare Information Management & Communications, Canada, April 2007. Available online at: http://www.healthcareimc.com/sites/default/files/previous/Volume%2021/Volume%2021%20Number%202/Health%20Service%20Provider%20Fined%2010,000.pdf

20 Available online at: https://pharmacists.ab.ca/sites/default/files/SonggadanDecision.pdf

21 Office of the Information and Privacy Commissioner of Alberta, *Conviction in Health Information Act Investigation*, April 2014. Available online at: http://oipc.ab.ca/downloads/documentloader.ashx?id=3405

22 Office of the Information and Privacy Commissioner, *Sentence Handed Down in Personal Health Information Act Matter*, September 2014. Available online at: http://www.releases.gov.nl.ca/releases/2014/oipc/0911n08.aspx

23 Office of the Information and Privacy Commissioner, *Sentence Handed Down in Personal Health Information Act Matter*, October 2014. Available online at: http://www.releases.gov.nl.ca/releases/2014/oipc/1009n09.aspx

In 2012, the Ontario Court of Appeal also recognized a new common law right of action for invasion of privacy, the tort of "intrusion upon seclusion."[24] To establish this cause of action, one must prove that the defendant's conduct is intentional or reckless; the defendant invaded the plaintiff's private affairs or concerns without lawful justification; and a reasonable person would regard the invasion as highly offensive, causing distress, humiliation or anguish. Proof of harm is not an element of the cause of action. The Court of Appeal stated that ordinarily the appropriate range of damages is a maximum of $20,000 and that aggravated and punitive damages may be appropriate in exceptional cases.[25]

Class action lawsuits are also becoming more prevalent in response to unauthorized access to personal health information. A $5.6 million class action lawsuit has been launched in Ontario claiming the tort of intrusion upon seclusion based on an allegation that 280 records of personal health information were intentionally and wrongfully accessed and, in a number of instances, improperly disseminated, without consent, by Peterborough Regional Health Centre and seven of its employees. The lawsuit is also seeking aggravated and punitive damages in the amount of $1 million from the hospital and $50,000 from each former employee.[26] A $412 million class action lawsuit has also been launched in Ontario after Rouge Valley Health System reported that former employees inappropriately used and/or disclosed the personal health information of up to 8,300 patients in order to sell or market RESPs. One of the former employees was also charged by the Ontario Securities Commission with unregistered trading, contrary to the *Securities Act*.[27]

Class action lawsuits have also been commenced elsewhere in Canada. In Newfoundland and Labrador and in Nova Scotia, class action lawsuits have been commenced against numerous health authorities after the plaintiffs were advised that their personal health information had been inappropriately accessed.[28]

---

24 *Jones v. Tsige*, 2012 ONCA 32 (CanLII) Available online at: http://www.canlii.org/en/on/onca/doc/2012/2012onca32/2012onca32.html

25 There is a decision pending before the Ontario Court of Appeal in which a hospital argued that plaintiffs are not able to bring an action based on the tort of intrusion upon seclusion because *PHIPA* confers exclusive jurisdiction on the Information and Privacy Commissioner of Ontario to resolve all claims related to the improper handling of personal health information subject to *PHIPA*. This decision is on reserve. For further information see *Hopkins v. Kay*, 2014 ONSC 321 (CanLII). Available online at: http://www.canlii.org/en/on/onsc/doc/2014/2014onsc321/2014onsc321.html

26 MyKawartha.com, *Class action lawsuit filed against hospital, former staff and Fleming College*, March 2013. Available online at: http://www.mykawartha.com/community-story/3715923-class-action-lawsuit-filed-against-hospital-former-staff-and-fleming-/ and *Hopkins v. Kay*, 2014 ONSC 321 (CanLII) http://www.canlii.org/en/on/onsc/doc/2014/2014onsc321/2014onsc321.html

27 Marco Chown Oved, Toronto Star, *Rouge Valley hospital clerk charged with misusing confidential patients records*, November 2014. Available online at: http://www.thestar.com/news/crime/2014/11/24/hospital_clerk_charged_with_misusing_records_after_confidential_patient_files_were_sold.html

28 Bob Buckingham Law, *Class Action Proceedings Initiated*. Available online at: https://www.buckinghamlaw.ca/index.php/lawsuits-filings/medical-records-privacy-breach; Patterson Law, *Class Proceeding Against Capital District Health Authority*. Available online at: http://www.pattersonlaw.ca/classproceedings/CapitalDistrictHealthAuthority/tabid/980/Default.aspx; and Wagners, *South West Health Privacy Breach*. Available online at: http://www.wagners.co/South-West-Health-Privacy-Breach//.

# PREVENTING OR REDUCING THE RISK OF UNAUTHORIZED ACCESS

Custodians are accountable for personal health information in their custody or control and for the actions of their agents with respect to that information. Unauthorized access to personal health information by agents with role-based access privileges is a known risk to personal health information in electronic information systems. Therefore, to fulfil their obligation to take steps that are reasonable in the circumstances to protect personal health information from unauthorized use or disclosure, custodians must take a multifaceted approach to detecting, preventing and reducing the risk of unauthorized access. A variety of measures should be implemented to combat unauthorized access including privacy policies and procedures, privacy training and awareness, privacy notices and privacy warning flags, confidentiality agreements, end-user agreements, access management, logging, auditing and monitoring, privacy breach management and discipline. Each of these measures is described below.

## PRIVACY POLICIES AND PROCEDURES

Custodians should develop and implement comprehensive privacy policies and procedures that set out the expectations and requirements for all agents. Written policies and procedures are necessary to formalize and clarify required practices. Privacy policies and procedures should be clearly written, readily accessible and easily understood. They should be endorsed by senior management, communicated throughout the organization and implemented consistently.

The privacy policies and procedures should be reflected in concrete practices and operationalized throughout the activities of an organization. For every requirement set out in the privacy policies and procedures, the custodian should consider how it can most effectively be achieved through a series of concrete, actionable and specific practices. These actionable items should clearly identify who is responsible for executing them and how each requirement will be met.[29]

Privacy policies and procedures should be in place to detect, prevent and reduce the risk of unauthorized access to personal health information by custodians and their agents. The purposes for which personal health information may be collected, used and disclosed and any limitations, conditions or

29 A *Policy is Not Enough: It Must be Reflected in Concrete Practices*, Office of the Information and Privacy Commissioner of Ontario, September 2012. Available online at: http://www.ipc.on.ca/English/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=1210

restrictions placed the collection, use and disclosure should be identified. As well, the purposes for which personal health information is not permitted to be collected, used or disclosed should be indicated. Privacy policies and procedures should specify that, as required under *PHIPA*, custodians and their agents must not collect, use or disclose personal health information if other information will serve the purpose and must not collect, use or disclose more personal health information than is reasonably necessary to meet the purpose. Privacy policies and procedures should also outline the responsibilities of custodians and their agents in relation to the administrative, technical and physical safeguards implemented to protect personal health information. The privacy policy and procedures should require agents to notify the custodian at the first reasonable opportunity if personal health information is stolen, lost or accessed by unauthorized persons. Comprehensive privacy policies and procedures should be in place, including, but not limited to, topics such as privacy training and awareness, execution of confidentiality agreements and end-user agreements, logging, auditing and monitoring, access management, privacy breach management and discipline.

All privacy policies and procedures should be reviewed regularly, at a minimum on an annual basis, to determine whether amendments are needed or whether new policies and procedures are required. The privacy policies and procedures should specify the frequency of the review, the person responsible for undertaking the review, the review procedure, and the time frame in which the review will be undertaken. In undertaking the review and in determining whether amendments and/or new privacy policies and procedures are necessary, it is important to have regard to any orders, guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario; evolving industry privacy standards and best practices; amendments to *PHIPA* and its regulations; recommendations arising from privacy and security audits, privacy impact assessments, threat risk assessments, and investigations into privacy complaints, privacy breaches and information security breaches. In addition, the review should ensure that the privacy policies and procedures continue to be consistent with actual practices and that there is consistency among the privacy policies and procedures implemented. Each privacy policy should also specify that agents must comply with the privacy policy and its procedures as well as how and by whom compliance will be enforced and the consequences of a breach.

## PRIVACY TRAINING AND AWARENESS

Comprehensive privacy training is an essential tool to reduce the risk of unauthorized access to personal health information. Custodians should ensure agents are provided with and are required to undergo initial and ongoing privacy training. As well, custodians should take steps to foster a culture of privacy

and raise awareness among agents of their responsibilities under *PHIPA* and its regulations and the privacy policies and procedures implemented.

Custodians should develop and implement a policy and procedures to ensure that all agents, regardless of their role, are required to complete privacy training before beginning their employment, contractual or other relationship with the custodian and before being given access to personal health information, as well as ongoing annual privacy training. The policy and procedures should set out the required minimum content of the initial and ongoing privacy training in order to ensure that privacy training is formalized and standardized. The policy and procedures should require the privacy training materials to be reviewed and updated on a regular basis and set out the frequency for such reviews and updates. Ideally, privacy training materials should be reviewed and updated on an annual basis. The policy and procedures should define who is responsible for developing the privacy training materials, for reviewing and refreshing the privacy training materials, and for providing the privacy training. The policy and procedures should also address the method or methods by which privacy training will be provided. Role-based privacy training helps to ensure that agents understand how to apply the privacy policies and procedures in their day-to-day employment, contractual or other responsibilities.

The policy and procedures should require privacy training to include, at a minimum:

- The purposes for which agents are permitted to collect, use and disclose personal health information;
- Any limitations, conditions or restrictions imposed by the custodian on the collection, use and disclosure of personal health information;
- The privacy policies and procedures that have been implemented by the custodian and the obligations imposed on agents arising from the privacy policies and procedures;
- The obligations imposed on agents under *PHIPA* and its regulations, including the duty to notify the custodian at the first reasonable opportunity if personal health information is stolen, lost or accessed by unauthorized persons and the procedure for doing so;
- Notice that audits of all collections, uses and disclosures of personal health information will be conducted;
- The potential consequences for the custodian arising from agents who collect, use or disclose personal health information in contravention of *PHIPA* and its regulations and/or in contravention of the privacy policies and procedures;

- The potential consequences that may be imposed on agents who collect, use or disclose personal health information in contravention of *PHIPA* and its regulations and/or in contravention of the privacy policies and procedures;
- The actual consequences that have been imposed on agents who have collected, used or disclosed personal health information in contravention of *PHIPA* and its regulations and/or in contravention of the privacy policies and procedures;
- The administrative, technical and physical safeguards implemented by the custodian to protect personal health information and the duties and obligations of agents in implementing the safeguards; and
- A discussion of the nature, purpose and key provisions of the confidentiality agreement that agents must sign and comply with.

The policy and procedures should require the privacy training materials to be reviewed and updated on a regular basis to address, at a minimum:

- Any orders, guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario under *PHIPA* or its regulations;
- Evolving industry privacy standards and best practices;
- The implementation of new technologies, programs or services;
- Amendments to *PHIPA* or its regulations, and new privacy policies and procedures or amendments to privacy policies and procedures implemented by the custodian; and
- Recommendations arising from privacy and security audits, privacy impact assessments, threat risk assessments, and investigations into privacy complaints, privacy breaches and information security breaches.

The policy and procedures should require that a log be maintained to document the attendance of custodians and their agents at both initial and ongoing privacy training. The policy and procedures should identify the person responsible for and the procedure to be followed in documenting attendance, identifying agents who do not attend the privacy training and ensuring that the privacy training is completed. As well, the consequences for failing to attend privacy training should be addressed. It is also helpful to provide agents with reference materials such as manuals, guides, checklists or charts to be retained after privacy training is completed. As well, copies of privacy policies and procedures should be provided or made readily available online.

While initial and ongoing privacy training is crucial, the development of a culture of privacy is also important and is dependent on a level of privacy awareness beyond training. Ongoing privacy communications are an important step in preventing or reducing the risk of unauthorized access to personal health information. The policy and procedures should identify the person responsible for promoting and fostering a culture of privacy and for raising privacy awareness and should set out the frequency, method and nature of the privacy communications. A communications plan should also be developed to frequently remind agents of the privacy policies and procedures implemented by the custodian and of the obligations imposed by these policies and procedures and by *PHIPA* and its regulations. This communications plan should highlight the duties imposed on agents in respect of access to personal health information and the consequences that may arise from unauthorized access. Methods of communication may include, for example, e-mails, newsletters and posters.

## PRIVACY NOTICES AND PRIVACY WARNING FLAGS

Privacy notices reminding custodians and their agents of their obligations and of the consequences of unauthorized access to personal health information in contravention of *PHIPA* and its regulations and in contravention of the privacy policies and procedures implemented, may also serve to prevent or reduce the risk of unauthorized access to personal health information.

Prior to accessing personal health information in an electronic information system, a privacy notice should be prominently displayed which, at a minimum:

- Sets out the purposes for which personal health information is permitted to be collected, used and disclosed;
- Requires custodians and their agents to acknowledge they will only collect, use and disclose personal health information for the purposes set out;
- Requires custodians and their agents to acknowledge they have read, understood and agree to comply with the privacy policies and procedures implemented;
- Requires custodians and their agents to agree to comply with their duties under *PHIPA* and its regulations; and
- Sets out the consequences for failing to comply.

Privacy warning flags can also serve as an important deterrent to unauthorized access to personal health information and can assist in logging, auditing and monitoring access. A privacy warning flag is an alert or advisory that is associated with an electronic record of an individual. It may be applied at the

request of the individual or when the individual has withheld or withdrawn his or her consent to the collection, use or disclosure of personal health information for health care purposes. These flags contain a warning to any agent who attempts to access the personal health information that access to the information is closely monitored and that an alert will be automatically generated and sent to the privacy office or other designated agent of the custodian each time the privacy warning flag is by-passed and personal health information is accessed. In our experience, the ability to place a flag on electronic records is an effective means of preventing and detecting unauthorized access to personal health information.

Individuals should also be made aware of their ability to place privacy warning flags on their electronic records of personal health information. For example, the written public statement of the custodian, which is required by *PHIPA*, could include a description of the privacy warning flag, how it can be requested and to whom this request should be directed.

## CONFIDENTIALITY AGREEMENTS

Requiring agents to sign confidentiality agreements on a regular basis may also help to prevent or reduce the risk of unauthorized access to personal health information. Confidentiality agreements require agents to acknowledge the privacy obligations and expectations, including the consequences of a privacy breach.

Confidentiality agreements should be signed at the start of the employment, contractual or other relationship with the custodian and on an annual basis thereafter. Confidentiality agreements should, at a minimum:

- Set out the purposes for which agents are permitted to collect, use and disclose personal health information and any limitations, conditions or restrictions placed on the collection, use and disclosure;
- Prohibit agents from collecting, using or disclosing personal health information if other information will serve the purpose and from collecting, using or disclosing more personal health information than is reasonably necessary to meet the purpose;
- Require agents to acknowledge that they have read, understood and agree to comply with the privacy policies and procedures implemented;
- Require agents to securely return all property of the custodian, including keys and records of personal health information, if any, at the conclusion of their employment, contractual or other relationship with the custodian;
- Specify that random audits will be conducted;
- Require agents to comply with *PHIPA* and its regulations;

- Require agents to notify the custodian at the first reasonable opportunity, in accordance with the privacy breach management policy and procedures, of an actual or suspected breach of the confidentiality agreement, *PHIPA* or its regulations, or the privacy policies and procedures; and
- Set out the consequences of a breach, for example disciplinary action including termination or suspension of the employment, contractual or other relationship with the custodian and, where applicable, a report to the agent's health regulatory college.

## END-USER AGREEMENTS

In order to help reduce the risk of unauthorized access, each electronic information system containing personal health information should be accompanied by an end-user agreement which sets out the roles and responsibilities of all parties who use the system. Custodians should ensure that their agents sign end-user agreements prior to obtaining access to personal health information in electronic information systems and, at a minimum, every year thereafter. End-user agreements should:

- Set out the purposes for which personal health information may be collected, used and disclosed in the electronic information system;
- Require custodians and their agents to acknowledge that they have read, understood and agree to comply with the privacy policies and procedures implemented in relation to the electronic information system;
- Require custodians and their agents to comply with *PHIPA* and its regulations;
- Require custodians and their agents to implement the administrative, technical and physical safeguards set out in the end-user agreement to protect personal health information in the electronic information system;
- Set out the consequences of a breach of the end-user agreement; and
- Require notification, in accordance with privacy breach management policy and procedures, if an actual or suspected breach has occurred or is about to occur.

## ACCESS MANAGEMENT

Restricting access to personal health information on a need-to-know basis will help to minimize the risk of unauthorized access. A policy and procedures should be in place to limit access to and use of personal health information

based on the need-to-know principle. The purpose of this policy and procedures is to ensure that, as required by *PHIPA*, personal health information is not collected, used or disclosed if other information will serve the purpose, and that no more personal health information is collected, used or disclosed than is reasonably necessary to meet the purpose.

The policy and procedures should identify the person responsible for and the process to be followed for granting initial role-based access to personal health information and for revising or revoking access to personal health information when the required level of access changes, for example, where the agent's employment, contractual or other relationship with the custodian is suspended or terminated or an agent's job functions change. The policy and procedures should also set out the different levels of role-based access that may be granted, as well as the requirements that must be satisfied before approving or denying a request for access.

If the agent only requires access to personal health information for a specified period of time, the policy and procedures should set out the process for ensuring that access and use of the personal health information is only permitted for that period of time.

The policy and procedures should require the custodian to maintain a log of agents who are granted access to personal health information and should identify the person responsible for maintaining the log. The log should, at a minimum, include the identity of the agent who was granted access; a description of the personal health information to which the agent has been granted access; the level of access granted; the date of approval; the date the access was provided; and the termination date, if applicable. The log should be reviewed on a regular basis to ensure that only those agents who require access to personal health information for the purposes of their job functions have access, and to ensure that agents do not have access to more personal health information than is reasonably necessary for their job functions.

The policy and procedures should also set out additional physical, technical and administrative measures to limit agents' access to personal health information. For example, password controls and search controls are two important measures that may help to minimize the risk of unauthorized access.

With respect to password controls, it is important to note that the detection of unauthorized access to personal health information can be thwarted if an agent uses the login credentials of another agent of the custodian to access personal health information. For example, in one case of unauthorized access, the physician was able to gain access to personal health information using the credentials of other agents who failed to log out of Alberta Netcare.[30] Strong

30 Information and Privacy Commissioner of Alberta, *supra*, note 14.

passwords are the first line of defense against unauthorized access to personal health information. Typically, strong login passwords do not contain any dictionary words and are comprised of a combination of eight or more letters, numbers and symbols, with 14 or more being ideal. Agents should also be prohibited from writing down or sharing their passwords and unique user IDs and should be required to change their passwords on a regular basis. Agents should also be required to log off from electronic information systems when they are no longer in use to reduce the risk that another agent will be able to use their login credentials to access personal health information for unauthorized purposes. Where appropriate, automatic system time outs can be in place where the system logs the user off or locks the computer screen after a short period of inactivity.

With respect to search controls, it is important to note that open-ended search functionality may facilitate unauthorized access to personal health information in electronic information systems. For example, in the privacy breach involving the use and disclosure of personal health information for the purpose of selling or marketing RESPs, agents of the hospital were able to obtain lists of women who had recently given birth by performing open-ended searches of a patient index. To prevent this, custodians should ensure that the amount of personal health information that is displayed as a result of a search query is limited, while still enabling agents to carry out their employment, contractual or other duties. Open-ended searches for individuals should be prohibited by the search functionality and search capabilities of electronic information systems containing personal health information. Ideally, electronic information systems should be configured to ensure that search criteria return only one record of personal health information. If that is not feasible, then electronic information systems should be configured so that no more than five records of personal health information are displayed as a result of a search query.

## LOGGING, AUDITING AND MONITORING

The logging, auditing and monitoring of all accesses to electronic records of personal health information is important to ensure the privacy of individuals and the confidentiality of their personal health information. The capacity to log all instances where personal health information is collected, used and disclosed by agents will enable custodians to respond to requests for information and complaints about the collection, use or disclosure of an individual's personal health information; to audit and monitor all collections, uses and disclosures of personal health information by all of their agents; and to investigate actual or suspected privacy breaches including cases of unauthorized access.

Logging, auditing and monitoring can be an effective deterrent to unauthorized access if all agents are made aware that all of their activities in relation to electronic records of personal health information will be logged, audited and

monitored on an ongoing, targeted and random basis, as described below. Agents should also be informed about the detection of previous instances of unauthorized access by other agents of the custodian and the discipline that was applied in those circumstances.

Custodians should develop a policy and procedures for logging, auditing and monitoring all electronic information systems containing personal health information. The policy should, at a minimum, require the custodian to ensure that all electronic information systems containing personal health information are capable of logging all instances where all or part of the information is collected, used and disclosed by all of their agents, as well as all instances where all or part of the information is collected, used or disclosed as a result of an override of a consent directive or the by-passing of a privacy warning flag.

With respect to the logging of all collections, uses and disclosures of personal health information, the policy and procedures should set out the types of logs that the custodian is required to create and maintain; the minimum content of each type of log; the minimum length of time each type of log must be retained; and the person responsible for retaining each type of log.

The policy and procedures should require the logs of all instances where all or part of the personal health information in an electronic information system is collected, used and disclosed to, at a minimum, identify:

- The individual to whom the personal health information relates;
- The type of personal health information that was collected, used or disclosed;
- The agent who collected, used or disclosed the personal health information; and
- The date, time and location of the collection, use and disclosure of the personal health information.

The policy and procedures should require the logs of all instances where all or part of the personal health information in an electronic information system is collected, used or disclosed as a result of an override of a consent directive or the by-passing of a privacy warning flag to also identify the purpose for the collection, use or disclosure of personal health information, if applicable. For example, where a consent directive is overridden with the express consent of the individual, this should be specified in the log.

For electronic information systems that are shared among custodians, the logs should also identify the custodian who provided the information to the shared electronic information system and the custodian on whose behalf the personal health information was collected, used or disclosed by the agent.

With respect to the auditing and monitoring of the logs, the policy and procedures should set out the types of auditing and monitoring that must be conducted using the logs; the procedure for each type of auditing and monitoring; the person responsible for each type of auditing and monitoring; the frequency with which each type of auditing and monitoring must be conducted; the criteria to be used for each type of auditing and monitoring; the procedure to be followed for reviewing and addressing the findings of the auditing and monitoring; and the procedure to be followed in the event that an actual or suspected privacy breach is identified.

The policy and procedures should require the custodian to conduct ongoing, targeted (reactive) and random (proactive) auditing and monitoring of the logs, as described below.

The policy and procedures should require ongoing auditing and monitoring to be conducted where a consent directive or a privacy warning flag has been implemented. Specifically, the policy and procedures should require that whenever personal health information is collected, used or disclosed as a result of an override of a consent directive or the by-passing of a privacy warning flag, an alert or notice be sent to the privacy office or other designated agent of the custodian on whose behalf the personal health information was collected, used or disclosed. The policy and procedures should require the privacy office or other designated agent to audit and monitor all instances where personal health information is collected, used or disclosed as a result of an override of a consent directive or the by-passing of a privacy warning flag to ensure compliance with an individual's consent preferences, and with *PHIPA*. The policy and procedures should also require the privacy office or other designated agent to notify the individual to whom the information relates each time personal health information is collected, used or disclosed as a result of an override of a consent directive or the by-passing of a privacy warning flag to help ensure compliance.

The policy and procedures should require targeted auditing and monitoring to be conducted in response to requests or complaints from individuals regarding the collection, use or disclosure of their personal health information, and whenever an actual or suspected privacy breach is identified.

The policy and procedures should also require the custodian to conduct random auditing and monitoring of all collections, uses and disclosures of personal health information by all of their agents. To deter and detect unauthorized access, random auditing and monitoring may include reviews of, for example, all agents who accessed an electronic information system during a specified period of time; all agents who accessed the personal health information of a specific individual, such as a celebrity, politician or other well-known individual, during a specified period of time; all agents who accessed the personal health

information of one or more individuals with the same last name as the agent (i.e., family members); and all individuals whose personal health information was access by a specific agent during a specified period of time.[31]

Third party audit tools are also available which can systematically and automatically analyze access logs and generate reports based upon defined search criteria. By automating manual processes, using a variety of queries based upon a custodian's specific requirements, third party tools can help ensure greater efficiency in audit reviews and enable more effective reviews of usage patterns. Specialized audit tools can help prevent and detect unauthorized access to personal health information by recording patterns of agents access and activity in electronic information systems, monitoring and analyzing agents' behaviour for patterns that could indicate misuse, and generating alerts or reports in order to contain unauthorized activity and to trigger further auditing.

## PRIVACY BREACH MANAGEMENT

With respect to privacy breaches, custodians and their agents are subject to a number of obligations set out in *PHIPA*. *PHIPA* requires custodians to take steps that are reasonable in the circumstances to ensure the personal health information in their custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure records containing personal health information are protected against unauthorized copying, modification or disposal. *PHIPA* also requires custodians to notify individuals at the first reasonable opportunity if their personal health information is lost, stolen or accessed by unauthorized persons. Agents are also required to notify the custodian at the first reasonable opportunity if personal health information handled by the agent on behalf of the custodian is stolen, lost or accessed by unauthorized persons.

In order to comply with their obligations under *PHIPA*, custodians should be able to respond quickly and effectively in the event that unauthorized access to personal health information is suspected or detected. Custodians should develop and implement a privacy breach management policy and procedures that addresses the identification, reporting, containment, notification, investigation and remediation of suspected or actual privacy breaches. Such a policy and procedures should enable a custodian to respond quickly and in a coordinated manner; clarify roles and responsibilities; document processes for effectively identifying, containing, investigating and remediating privacy breaches; ensure that individuals, senior management, and potentially other

31 *Preventing/Reducing Unauthorized Access to Personal Health Information*, Ontario Hospital Association and the Office of the Information and Privacy Commissioner of Ontario, November 2012. Available online at: http://www.oha.com/KnowledgeCentre/Library/Documents/Final%20-%20PHIPA%20Primer.pdf

third parties are informed about privacy breaches; and prepare the custodian for potential involvement by the Information and Privacy Commissioner of Ontario.[32]

The privacy breach management policy and procedures should impose an obligation on agents to notify the custodian if personal health information is stolen, lost or accessed by unauthorized persons and identify who within the organization should be notified and the time frame for notification. It should require agents to report a privacy breach to senior management and set out who is responsible for such reporting, the time frame within which this reporting should be completed and to whom the privacy breach should be reported. It should also set out the circumstances in which a privacy breach must be reported to others including police, health regulatory colleges and the Information and Privacy Commissioner of Ontario.

The privacy breach management policy and procedures should require steps that are reasonable in the circumstances be immediately taken in order to contain the privacy breach and to protect personal health information from further theft, loss or unauthorized use or disclosure and to protect records of personal health information from further unauthorized copying, modification or disposal. In cases of unauthorized access, custodians should take all steps necessary to contain the privacy breach, such as immediately suspending access to personal health information by the agent suspected of the privacy breach, pending the outcome of an investigation. Custodians should retrieve all hard copies of personal health information that have been disclosed and should ensure that no copies have been made or retained by unauthorized persons. The custodian should determine whether the privacy breach would allow the unauthorized collection, use or disclosure of any other personal health information and take steps to ensure that additional privacy breaches cannot occur through the same or similar means.

The privacy breach management policy and procedures should require notification of affected individuals pursuant to *PHIPA*, and set out who is responsible for providing notification and the information to be provided.

When notifying individuals about a privacy breach, custodians should provide individuals with the following information:

- The name of each agent who caused the privacy breach;
- The date and time of the privacy breach;
- A description of the nature and scope of the privacy breach;
- A description of the personal health information that was subject to the privacy breach;

32 *What to do When Faced With a Privacy Breach: Guidelines for the Health Sector*, Office of the Information and Privacy Commissioner of Ontario. Available online at: http://www.ipc.on.ca/images/Resources/hprivbreach-e.pdf

- The measures implemented to contain the privacy breach;
- Notice that, following the investigation, the custodian will provide the individual with a summary of the results of the investigation and the measures that have been or will be implemented to remediate the privacy breach and to prevent similar privacy breaches in the future;
- The steps the individual can take to protect his or her privacy or to minimize the impact of the privacy breach;
- The name and contact information for the person to whom the individual may address inquiries and concerns; and
- Information concerning how to make a complaint to the Information and Privacy Commissioner of Ontario.

The privacy breach management policy and procedures should require that an investigation of the privacy breach be conducted including a review of all relevant electronic information systems and privacy policies and procedures; set out who is responsible for conducting the investigation, the nature and scope of the investigation and the process to be followed in conducting the investigation; and set out the process by which the findings of the investigation, including any recommendations, are communicated and implemented, the time frame for implementation and the person responsible for implementation.

After completing the investigation, the privacy breach management policy and procedures should require the custodian to provide the individual with a summary of the results of the investigation and the measures that have been or will be implemented to remediate the privacy breach and to prevent similar privacy breaches in the future.

The privacy breach management policy and procedures should require the custodian to keep a log of privacy breaches and set out the content of the log and identify the person responsible for maintaining the log. The log should include for each privacy breach:

- The name of the agent that caused the privacy breach, where it is determined to be relevant such as in the case of unauthorized access;
- The date and time of the privacy breach;
- The nature, scope and cause of the privacy breach;
- A description of the personal health information that was subject to the privacy breach;
- The measure implemented to contain the privacy breach;
- The measures that have been or will be implemented to remediate the privacy breach and to prevent similar privacy breaches in the future;

- The timelines and persons responsible for implementing measures to remediate the privacy breach and prevent similar privacy breaches in the future; and
- The manner in which each measure was or is expected to be implemented.

The privacy breach management policy and procedures should require the custodian to audit and monitor the log of privacy breaches to identify patterns or trends in privacy breaches; to identify administrative, physical or technical safeguards that should be implemented to prevent or minimize the risk of privacy breaches; and to ensure that measures to remediate the privacy breaches and prevent similar privacy breaches in the future are implemented. For example, if the custodian detects an increase in the frequency of privacy breaches involving unauthorized access to personal health information, this may trigger a review of the custodian's logging, auditing and monitoring policies and procedures or the discipline imposed for such privacy breaches.

## DISCIPLINE

Imposing consistent, appropriate and proportionate discipline lets agents know that privacy breaches are taken seriously and can serve as an effective deterrent against unauthorized access to personal health information. Custodians should have a policy and procedures regarding discipline and corrective action. The policy and procedures should address the investigation of disciplinary matters; the types of discipline and corrective action that may be imposed, for example, a warning letter, suspension with or without pay, and termination of the employment, contractual or other relationship with the custodian; the circumstances in which the actions of agents will be reported to third parties including the police, their health regulatory college and/or the Attorney General to commence a prosecution under *PHIPA*; and the factors to be considered in determining the appropriate discipline and corrective action.

Agents should be informed of the discipline policy and procedures of the custodian, as well as the potential consequences for unauthorized access to personal health information under *PHIPA*. For example, agents may be informed about discipline and other consequences of unauthorized access through privacy training, privacy awareness communications, and by signing confidentiality agreements containing provisions related to discipline. Agents should be informed of specific examples of privacy breaches that have occurred within the organization and of the ensuing discipline that has been imposed. Repeatedly reminding agents that there is no tolerance, both in policy and practice, for unauthorized access to personal health information can serve to deter and prevent privacy breaches.

# CONCLUSION

Unauthorized access to personal health information by custodians and their agents appears to be a prevalent problem. The negative consequences stemming from unauthorized access are extensive and far-ranging. Unauthorized access to personal health information may cause harm to individuals and irreparably damage the trust relationships between custodians and the individuals to whom they provide health care. Other potential ramifications of unauthorized access include disciplinary proceedings, privacy investigations and orders, prosecutions for offences under *PHIPA*, and lawsuits.

It is important that custodians and their agents recognize that the issue of unauthorized access to personal health information, regardless of motive, is significant and is taken seriously. The protection of privacy should be integral to the delivery of health care and embedded into the culture of health care organizations. Developing and implementing a comprehensive approach, incorporating a variety of measures and ensuring agents are aware of the relevant privacy policies and procedures can go a long way toward minimizing the risk of unauthorized access to personal health information. A strong message should be sent that unauthorized access to personal health information by custodians and their agents is not acceptable and will not be tolerated and those who do so may face serious consequences.

# DETECTING, PREVENTING AND REDUCING THE RISK OF UNAUTHORIZED ACCESS

1. Develop and implement comprehensive privacy policies and procedures that set out the expectations and obligations of all agents for the protection of personal health information.

2. Develop and implement a comprehensive privacy training and awareness program which requires all agents to complete privacy training at the beginning of their employment, contractual or other relationship with the custodian and before being granted access to personal health information, as well as ongoing annual privacy training, to ensure agents understand the expectations and obligations for the protection of personal health information under the privacy policies and procedures of the custodian as well as under *PHIPA*.

3. Ensure that electronic information systems that contain personal health information in the custody or control of the custodian include privacy notices and privacy warning flags.

4. Require all agents to sign confidentiality agreements, before being granted access to personal health information and on annual basis thereafter, to acknowledge the privacy expectations and obligations for the protection of personal health information under the privacy policies and procedures of the custodian as well as under *PHIPA*.

5. Require all agents to sign end-user agreements acknowledging the expectations and obligations that apply to personal health information in electronic information systems before being granted access and on an annual basis thereafter.

6. Develop and implement comprehensive policies and procedures and physical, technical and administrative measures, such as password controls and search controls, to limit access to and use of personal health information by agents based on the need-to-know principle.

7. Ensure that all accesses to personal health information in electronic information systems are logged, audited and monitored on an ongoing, targeted (reactive) and random (proactive) basis.

8. Develop and implement a comprehensive privacy breach management policy and procedures that address the identification, reporting, containment, notification, investigation and remediation of suspected or actual privacy breaches.

9. Develop and implement a policy and procedures that sets out the types of discipline or corrective action that may be imposed on agents for privacy breaches, including termination of the employment, contractual or other relationship with the custodian and the circumstances in which the actions of agents may be reported to third parties including the police, their health regulatory college and/or the Attorney General to commence a prosecution under *PHIPA*.

## ABOUT THE INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO

**The role of the Information and Privacy Commissioner of Ontario is set out in three statutes: the *Freedom of Information and Protection of Privacy Act*, the *Municipal Freedom of Information and Protection of Privacy Act* and the *Personal Health Information Protection Act*. The Commissioner acts independently of government to uphold and promote open government and the protection of personal privacy.**

**Under the three Acts, the Commissioner:**

- **Resolves access to information appeals and complaints when government or health care practitioners and organizations refuse to grant requests for access or correction;**
- **Investigates complaints with respect to personal information held by government or health care practitioners and organizations;**
- **Conducts research into access and privacy issues;**
- **Comments on proposed government legislation and programs; and**
- **Educates the public about Ontario's access and privacy laws.**

Information and Privacy
Commissioner of Ontario

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

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario
Canada M4W 1A8

Web site: www.ipc.on.ca
Telephone: 416-326-3333
Email: info@ipc.on.ca

January 2015