Personal Health Information:

A Practical Tool for Physicians Transitioning from Paper-Based Records to Electronic Health Records

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

Peter G. Rossos, MD, MBA, FRCP(C), FACP
Chief Medical Information Officer
UHN & SIMS Partnership

May 21, 2009

Dr. Ann Cavoukian, the Information and Privacy Commissioner of Ontario, gratefully acknowledges the work of Debra Grant in preparing this report.

Dr. Peter G. Rossos is an Associate Professor of Medicine, Division of Gastroenterology, University of Toronto.

Information and Privacy
Commissioner of Ontario

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

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

Table of Contents

Abstract

There is increasing pressure on the health-care sector to accelerate the conversion from paper-based records to electronic health records. Electronic systems of personal health information offer many benefits to practitioners and patients. For example, they support improved clinical decision-making leading to more effective diagnosis and treatment, greater patient safety, increased efficiency and improved access to services. On the downside, however, electronic systems pose unique risks to the privacy and security of personal health information. These risks can be minimized through careful consideration of the risks during the design and implementation of these systems.

Since paper-based and electronic records each have their own privacy and security risks, personal health information may be at its greatest risk of exposure to privacy and security breaches when physicians are making the transition from paper-based records to electronic records. The present toolkit has been prepared by the Office of the Information and Privacy Commissioner of Ontario (IPC) and Dr. Peter Rossos of the University Health Network, to help physicians minimize the risk of privacy and security breaches before, during and after making the transition to electronic records of personal health information.

The toolkit explains why privacy is so important in the delivery of health-care and briefly describes the various types of electronic records of personal health information that physicians may opt to employ in their practices. It outlines the general obligations that physicians have to protect personal health information and those specific to electronic systems. It describes the privacy and security issues that must be considered in making the transition, in using electronic records of personal health information, and in managing paper-based records after making the transition to electronic systems. Finally, the toolkit provides some general guidance on how to address the privacy and security issues, and refers physicians to several useful resources for more detailed information.

While the challenges outlined in the paper may seem considerable, physicians who have made this transition successfully confirm that they are not insurmountable and the benefits that accrue following the transition make it well worth the effort.

Introduction

> *All that may come to my knowledge in the exercise of my profession or in daily commerce with men, which ought not to be spread abroad, I will keep secret and will never reveal.*
>
> *Hippocratic Oath*

Health information is a unique type of personal information. On the one hand, it is extremely sensitive, requiring the strongest privacy and security protections to prevent unauthorized use and disclosure. On the other hand, it must be readily available to a broad range of health-care providers for the purposes of delivering health-care to the individual. This binary nature of personal health information poses unique challenges for physicians making the transition from paper-based records to electronic systems of personal health information.

There is increasing pressure on the health-care sector to accelerate the conversion from paper-based records to electronic health records. The recently signed U.S. stimulus bill mandates the use of electronic health records for each person in the U.S. by 2014. The bill designates $19 billion for health-care information technology, with the bulk of this money going toward incentives for physicians and hospitals to use electronic systems. Here at home, Canada Health Infoway has a core objective to provide electronic health records to 50 per cent of Canadians by 2010, while the Province of Ontario has committed to implementing a comprehensive electronic health record by 2015. In addition, as private corporations, such as Google and Microsoft, expand their efforts to provide services and tools for patients to manage their own personal health information online, patients will increasingly demand and expect their health-care providers to make this information available electronically.

Electronic systems of personal health information offer many benefits to practitioners and patients. In general, paper-based records may be incomplete, spread over a range of health-care provider locations, and difficult to locate and read. In contrast, a shared electronic record of personal health information may be readily accessed by all of the individuals' health-care providers, regardless of where they are located. It is also more likely to contain complete and up-to-date personal health information about an individual. An electronic record requires less space and fewer administrative resources to maintain. It supports improved clinical decision-making leading to more effective diagnosis and treatment, greater patient safety, increased efficiency and improved access to services.

With electronic records of personal health information, there is the potential for automating, structuring and streamlining clinical workflow and integrating a wide range of discrete health-care services including decision support, patient monitoring, electronic prescribing, electronic referrals, radiology, laboratory ordering and results display. Electronic health information systems can also provide a data trail that can be readily used for the purposes of medical audit, health research, quality assurance, epidemiological monitoring and disease surveillance.

The use of information technology in physicians' offices is rapidly becoming a necessity – physicians must make this transition to keep pace with the modern health-care system. It is no longer a question of whether or not physicians will make this transition, but rather when. As the provision of health-care becomes increasingly complex, involving a wide range of health-care providers and the use of sophisticated diagnostic tests and specialized treatment, physicians will need to rely on technology to help them manage their patients' care in an efficient and effective manner. In addition, information technology is essential for physicians to fully benefit from the pay-for-performance incentive programs that are being introduced in Ontario as a means of improving the quality of patient care. These incentive programs allow physicians, participating in primary care programs, to receive bonuses for ensuring that patients on their roster participate in screening or prevention programs involving mammography, Pap tests, childhood vaccinations, flu shots, and fecal occult blood testing. Electronic medical records can provide prompts and/or recall notices when an intervention is overdue, and this helps to ensure that physicians meet their specified targets. For example, from 2007 to 2008, 11 physicians from one family practice in Ottawa reported exceeding the target goals by as much as 16 per cent and exceeding U.S. diabetes-management targets in areas such as blood pressure and LDL cholesterol levels through the use of electronic medical records.[1]

On the downside, however, electronic systems may pose unique risks to the privacy and security of personal health information. This is because they not only allow for the collection, use and disclosure of massive amounts of personal health information from diverse sources at the press of a key, but they are more likely to attract hackers and others with malicious intent. The good news, however, is that with careful consideration of the privacy and security implications, electronic systems of personal health information can be designed and implemented in a manner that addresses these risks. In fact, through the use of encryption, access controls, audit logs and other tools, enhanced privacy and security can be attained for electronic records. We call this *Privacy by Design*[2] — when privacy and security safeguards are built directly into a new information system or other technology, thereby ensuring the greatest protection.

While concern about the potential risks is often cited as a reason to delay the implementation of electronic health records, it is important to point out that paper-based records also have their own privacy and security vulnerabilities. Numerous high profile privacy breaches have occurred due to the improper collection, use, disclosure, retention or disposal of paper-based records. For example, in one case, paper-based records that were not disposed of, in a secure manner, ended up being used as props on a movie set and strewn across a street in downtown Toronto. In another case, laboratory reports ended up in a dumpster outside a medical building. Ironically, these paper-based records were being disposed of by the laboratory because the health-care providers, who requisitioned the laboratory tests, use electronic health records and are not interested in receiving hard copies of laboratory results. In other cases, sensitive medical information has been transmitted via facsimile to the wrong number.

1 See "More electronic medical records mean more preventive care, conference told," published on May 16, 2008 on the website of the Canadian Medical Association at www.cma.ca.

2 *Privacy by Design*, an approach developed in the 90s by Dr. Ann Cavoukian, seeks to systematically build privacy into information technologies, systems and architectures, at the design stages.

Since paper-based and electronic records each have their own privacy and security challenges, personal health information may be at its greatest risk of exposure to breaches when physicians are making the transition from paper-based records to electronic records. Many factors converge to increase this risk. First, during this transition phase, staff may not be fully trained on using the new electronic system, greatly increasing the likelihood of human errors. Second, during the initial implementation phase, the new electronic system may not be fully functional – the privacy and security features of the system may be either turned off or set to the minimal standard of protection, until the user modifies the default settings. Third, the conversion of existing paper-based records to electronic format may require more frequent access to records of personal health information by a broader range of persons than would normally be the case. Fourth, records may be duplicated in electronic format *and* paper-based format, potentially doubling the volume of records that need to be protected. Fourth, the archiving, retention and disposal of paper-based records, if not carried out in a secure manner, may also pose a threat to privacy. Finally, physicians may require assistance from third party service providers to make the transition, adding an additional layer of complexity to the privacy and security risks that must be managed.

In addition, the potential inaccessibility of records during the transition phase may introduce risks that go well beyond the privacy and security of the personal health information. For example, the lack of readily available paper-based and/or electronic records may interrupt normal workflows within a physician's office and pose risks to patient safety. To minimize exposure to these risks, it is important to limit the transition phase to the shortest time possible through careful planning and preparation. In addition, physicians may want to consider interim solutions, such as scanning all paper-based records and storing them electronically, to ensure their availability during the transition phase.

The present toolkit has been prepared by the Office of the Information and Privacy Commissioner of Ontario (IPC) and Dr. Peter Rossos of the University Health Network (UHN), to help physicians minimize the risk of privacy and security breaches before, during and after making the transition to electronic records of personal health information. While the challenges presented in this toolkit may seem daunting, physicians who have successfully made this transition agree that the challenges are definitely surmountable and the benefits that accrue following the transition make it well worth the effort.

The toolkit explains why privacy is so important to the delivery of health-care and briefly describes the various types of electronic records of personal health information that physicians may opt to employ in their practices. It outlines the general obligations that physicians have to protect personal health information and those specific to electronic systems. It describes the privacy and security issues that must be considered in making the transition, in using electronic records of personal health information, and in managing paper-based records after making the transition to electronic systems. Finally, the toolkit provides some general guidance on how to address the privacy and security issues and refers physicians to several useful resources for more detailed information.

Why is Privacy Protection So Important in Health Care?

Regardless of whether health-care providers use paper-based systems or electronic systems of health information, it is essential that patients trust that their privacy will be protected when they seek health-care. Research has shown that if patients have concerns about the inappropriate use and disclosure of their personal health information, they will engage in certain self-protective behaviours to protect their privacy. In 2005, the California HealthCare Foundation found that one in eight patients reportedly engages in behaviour to protect personal privacy, presenting a potential risk to their health.[3] These behaviours include asking a physician to forego reporting a health problem or to report a less serious diagnosis, avoiding their regular physician for certain health conditions, avoiding diagnostic tests due to anxiety over their privacy, and paying out of pocket for procedures to avoid submitting a claim. More than half of respondents also reported being concerned that employers may use their health information to limit job opportunities. Yet despite these concerns, consumers report a favourable view of new health information technology, with a majority (59 per cent) willing to share personal health information when it could result in better medical treatment. Similarly high levels of support for electronic health records have been found among Canadians.[4]

To the extent that patients lack trust and engage in behaviours to protect their privacy, the health information that is collected by their health-care providers may be inaccurate and incomplete. Health-care is an information-intensive industry. The delivery of high quality health-care depends on the availability of accurate and complete health information. Accurate and complete data is also essential for conducting high quality health research and for the effective planning and management of our publicly-funded health-care system. In short, a great deal rests with the accuracy and quality of the health information obtained, which in turn, rests on the confidence that patients have regarding the protection of their most sensitive information.

Electronic Patient Information

Physicians may rely on a number of different types of systems of electronic health records in their practices. It is important that physicians understand the differences between these systems and the privacy and security risks associated with each type. For the purposes of this toolkit, a distinction will be made among shared electronic health records (EHRs), electronic medical records (EMRs) and electronic personal health records (PHRs).

Canada Health Infoway, Canada's catalyst for collaborative change to accelerate the use of electronic health information systems and EHRs, defines an EHR as a secure and private lifetime record of an individual's health and care history. It provides authorized health-care

3 California HealthCare Foundation, National Consumer Health Privacy Survey 2005, Forrester Research, Inc. available at http://www.chcf.org/.

4 *Electronic Health Information and Privacy Survey: What Canadians Think – 2007* was prepared by EKOS Research Associates on behalf of Canada Health Infoway, Health Canada, and the Office of the Privacy Commissioner of Canada.

professionals with immediate access to their patients' health histories, including laboratory and radiology test results, past treatments, prescription drug profiles and immunizations.

While the terms EHR and EMR are often used interchangeably, for the purposes of this toolkit, the term EMR will be used to refer to an electronic system of patient records that is used by one health-care provider or facility. It only includes information about the care provided to the patient by their physician (akin to their paper-based file), a particular health-care provider or a health-care facility. In contrast, the EHR integrates information about the patient's care provided by *all* of the patient's health-care providers, over the course of the patient's life.

A more recent trend is the development of applications that enable patients to create, review, annotate, or maintain an electronic record of any aspect(s) of their own health condition, medications, medical problems, allergies, vaccination history, visit history, or communications with their health-care providers. For the purposes of this toolkit, this type of application will be referred to as a personal health record (PHR). For example, Microsoft currently offers an internet-based consumer health platform for developing PHRs referred to as HealthVault; Google offers a similar product referred to as Google Health. In addition, some health-care facilities allow patients to access to their own EMRs through patient portals. One example is "MyChart" offered by Sunnybrook Hospital in Toronto. In contrast to PHRs which are created and controlled by patients, patient portals generally offer a window or gateway to personal health information maintained by a health-care provider or facility.

The newly created agency, eHealth Ontario, that brings together the Ministry of Health and Long-Term Care's ehealth office and the Smart Systems for Health Agency under one umbrella, is responsible for all province-wide ehealth initiatives, including the development of an interoperable EHR. As noted by the recently appointed CEO of the new eHealth Ontario agency, Sarah Kramer:

> *I know from my experience with the Wait Times Strategy and Computerized Physician Order Entry (CPOE) for Chemotherapy that physicians are eager to use electronic tools to gain access to better information to improve care and to deliver better, faster service to their patients. While electronic health records potentially increase the scope of health information available to physicians, and, therefore, to unauthorized system users, these electronic tools can also offer greater privacy protections for patients. For example, the Wait Time Information System has electronic audit features that do not exist with paper records. For physicians transitioning their records from paper to electronic systems, we need to ensure they have the tools they need to understand the different privacy risks they face in an electronic environment and, most importantly, to use security controls built into the system to mitigate privacy issues.*

General Obligation to Protect Personal Health Information

Regardless of what type of records are being used, health-care providers have a duty to ensure that personal health information is protected at all times. Ontario's *Personal Health Information Protection Act* (*PHIPA*) requires health information custodians, including physicians, to take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure, and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal. Health information custodians must notify the individual at the first reasonable opportunity if the information is stolen, lost or accessed by unauthorized persons. Health information custodians must also ensure that records of personal health information in their custody or control are retained, transferred and disposed of in a secure manner.

A recent study conducted in the United States found that state privacy regulation restricting hospital release of personal health information can reduce EMR adoption by hospitals by more than 24 per cent. [5] One of the main incentives for hospitals to implement EMRs is to avoid expensive duplicate tests. Thus, where one hospital adopts an EMR, there are large financial incentives for other nearby hospitals to follow suit. However, this "network effect" can potentially be suppressed by the existence of state privacy legislation. The authors presented evidence that suggests that this may be due to the increase in compliance costs associated with requirements for additional documentation, where information is shared outside a health-care facility.

Physicians should note that Ontario's *Personal Health Information Protection Act* was specifically designed so that it would not present a barrier to the disclosure of personal health information among health-care providers. *PHIPA* permits all health information custodians, including physicians, to collect, use and disclose personal health information for the purposes of providing health-care or facilitating the provision of health-care to the individual on the basis of *implied* or *assumed implied* consent. In the context of health-care, *PHIPA* does not require additional documentation, such as written patient consent, when personal health information is released outside of the health information custodian.

Regardless of the type of records that are used, *PHIPA* requires health information custodians to:

- appoint a contact person who is accountable for privacy matters;
- make available to the public a written statement setting out the custodian's information practices;
- ensure that their agents (i.e., employees and other persons acting on their behalf) only collect, use and disclose personal health information as permitted by the custodian and in accordance with the rules set out in *PHIPA*;

5 Amalia R. Miller and Catherine Tucker, *Privacy protection and technology diffusion: The case of electronic medical records*, available at http://ssrn.com/abstract=960233.

- ensure that personal health information is only collected, used and disclosed with the consent of the individual or as permitted by *PHIPA*; and
- provide individuals with the ability to access and request correction of their own personal health information.

If a physician chooses not to designate a contact person, then the physician must perform the functions of the contact person which include:

- Facilitating compliance with *PHIPA*;
- Ensuring that all agents are appropriately informed of their duties under *PHIPA*;
- Responding to inquires from the public about the physician's information practices;
- Responding to requests for access to or correction of records of personal health information; and
- Receiving complaints from the public about alleged contraventions of *PHIPA*.

The IPC has issued a fact sheet, *Safeguarding Personal Health Information*, highlighting a number of important safeguards for protecting personal health information. This fact sheet is available on the IPC website at www.ipc.on.ca.

As highlighted in the fact sheet, regardless of whether medical records are paper-based or electronic, physicians must take reasonable steps to keep personal health information securely stored. What is reasonable varies depending on the sensitivity of the information and the risks to which it is exposed. The size of an organization is also a factor to consider. For instance, large organizations dealing with significant amounts of sensitive personal health information will need to employ different security measures than small offices. Physicians must therefore scale their security measures to fit their own circumstances.

Steps to ensure safe storage of personal health information should address physical security, technological security and administrative controls. Physical security would include the use of locked filing cabinets, restricted office access, and alarm systems. Technological security would include the use of user IDs and passwords, encryption, firewalls, and virus scanners. Administrative controls would include concise, written security policies and procedures; the appointment of a staff member with overall responsibility for security; staff training; security clearances; access restrictions; regular audits of actual practices for compliance with security policies; and written confidentiality agreements.

Physicians must ensure that all records are stored in a secure area where they may only be accessed by those with a legitimate need to know. Non-medical staff, such as maintenance staff, should not be able to access any records of personal health information; those with a need to access records should be bound by an appropriate confidentiality agreement.

For more detailed information, physicians should consult additional resources such as the *Physician Privacy Toolkit*.[6]

Requirements Specific to Electronic Systems

PHIPA contains a number of provisions relating to electronic transactions. Specifically, health information custodians who use electronic means to collect, use, modify, disclose, retain or dispose of personal health information are required to comply with the prescribed requirements. While no regulations have been prescribed, following the mandatory three-year review of *PHIPA*, the Standing Committee on Social Policy recommended that the legislature amend *PHIPA* to permit the development of a broad range of regulations relating to ehealth. Thus, regulations relating to electronic health records are expected in the near future and physicians are advised to keep abreast of legislative developments in this area.

While legislated requirements have yet to be developed, the IPC fact sheet, *Safeguarding Personal Health Information*, suggests that, where electronic health records are kept, custodians should ensure the following:

- The use of features such as strong passwords to prevent unauthorized access;
- The installation of automatic backup for file recovery to protect records from loss or damage; and
- The creation and maintenance of an audit trail that, at a minimum:
    - Records the date and time of each entry for each patient;
    - Shows any changes made to the record; and
    - Preserves the original content when a record has been changed, updated or corrected.

Ontario Regulation 114/94 made under the *Medicine Act* states that the medical records required by regulation may be made and maintained in an electronic computer system only if it has the following characteristics:

1. The system provides a visual display of the recorded information.
2. The system provides a means of access to the record of each patient by the patient's name and, if the patient has an Ontario health number, by the health number.
3. The system is capable of printing the recorded information promptly.
4. The system is capable of visually displaying and printing the recorded information for each patient in chronological order.

6 The Toolkit was developed in conjunction with the Ontario Medical Association, the Ontario Hospital Association, the Ontario Hospital eHealth Council and the Information and Privacy Commissioner of Ontario.

5. The system maintains an audit trail that,
    1. records the date and time of each entry of information for each patient,
    2. indicates any changes in the recorded information,
    3. preserves the original content of the recorded information when changed or updated, and
    4. is capable of being printed separately from the recorded information for each patient.
6. The system includes a password or otherwise provides reasonable protection against unauthorized access.
7. The system automatically backs up files and allows the recovery of backed-up files or otherwise provides reasonable protection against loss of, damage to, and inaccessibility of, information.

Sharing Responsibility

When a physician implements an EMR or provides patients with access to a PHR, the physician will be responsible for ensuring the privacy and security of electronic health information. Where a shared EHR is being implemented, responsibility for its privacy and security will be shared among all health information custodians who access the shared record. It is important to note that a physician's obligation to protect personal health information does not end when that information is made available to other health-care providers through a shared EHR. This means that physicians will have to ensure that there is an effective governance structure and contractual agreements that clearly specify the roles and responsibilities of each party involved in developing, implementing and using the shared electronic record.

Making the Transition to Electronic Records

Privacy Impact Assessments

Depending on the circumstances, there are a number of steps that a physician may take to prepare for implementing a new electronic system. A privacy impact assessment (PIA), in this case involving health information, is a formal risk management tool used to identify the actual or potential effects that a proposed or existing information system, technology or program may have on patients' privacy. A PIA also identifies ways in which any privacy risks identified may be mitigated.

Although *PHIPA* does not require physicians to conduct PIAs, the IPC encourages physicians and other health information custodians to consider conducting PIAs whenever they are adopting a new information technology, such as an EMR, EHR or PHR. We recognize, however, that a PIA may not be necessary and/or feasible in all circumstances. While conducting a PIA is becoming a best privacy practice when implementing new information technology, in deciding whether or not a PIA is necessary, physicians should take into consideration the amount and sensitivity of the personal health information that will be migrated to the new system and the risks to which the information will be exposed. For example, systems that are implemented to facilitate the sharing of personal health information among a range of custodians may have higher privacy and security risks than systems that are intended to be used only within one health-care organization. Where the privacy and security exposure risks are higher, the need for a PIA is stronger.

For guidance on how to conduct a PIA, please refer to the paper, *Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act*, available on the IPC's website at www.ipc.on.ca.

Technical and Administrative Assistance

Making the transition from paper-based to electronic records of personal health information is a resource-intensive activity. Once decisions have been made about what hardware and software to purchase or lease, physicians will have to ensure that they have sufficient human resources and expertise to implement the new technology, enter personal health information into the new system, educate and train staff, and manage old paper-based records. We well appreciate the amount of time and resources that will need to be devoted to complete this exercise.

Agents of the Physician

During and after the transition, physicians may choose to rely on their own employees or other third parties to provide technical expertise, administrative support (e.g., data entry), records storage, and records disposal. Viewed as "agents" of physicians (under *PHIPA*), these third parties are only permitted to collect, use, disclose, retain or dispose of personal health information on the physician's behalf if the physician is permitted or required to do so, and the collection, use, disclosure, retention or disposal of the information is in the course of the agent's duties and not contrary to the limits imposed by the physician, *PHIPA* or another law. Agents are also required under *PHIPA* to notify the physician at the first reasonable opportunity if personal health information handled by the agent on behalf of the physician is stolen, lost or accessed by unauthorized persons. Physicians are responsible for ensuring that their agents are aware of these obligations. This may be accomplished through the development of clearly written privacy and security policies and procedures; privacy and security training; confidentiality agreements; and third party service agreements.

Electronic Service Suppliers

PHIPA also contains a number of provisions for persons who, while not considered "agents," nonetheless supply goods and services for the purpose of enabling a health information custodian to use electronic means to collect, use, modify, disclose, retain or dispose of personal health information. Generally, such service providers:

- Must not use any personal health information to which they have access, except as necessary in the course of providing the services;
- Must not disclose any personal health information to which they have access;
- Must not permit persons acting on their behalf to access information, unless the person agrees to comply with the restrictions placed on electronic service providers.

Health Information Network Providers

Other requirements under *PHIPA* apply to one specific type of provider referred to as a "health information network provider." A health information network provider refers to a person who provides services to two or more health information custodians, where the services are provided primarily to enable the custodians to use electronic means to disclose personal health information to one another, whether or not the person is an agent of any of the custodians. (Therefore a health information network provider need not be an agent of the custodian). In general, a health information network provider is required to:

- Notify every applicable health information custodian if there has been a privacy breach;
- Provide to each applicable health information custodian a plain language description of the services provided, including a general description of the safeguards in place to protect personal health information;
- Make available to the public the plain language description of the services provided, as well as any directives, guidelines and policies relating to these services, and a general description of the safeguards implemented by the service provider;
- Make available to each applicable health information custodian, upon request, an electronic record of all access to all or part of the personal health information and all transfers of all or part of the information associated with the custodian;
- Perform and provide, to each applicable health information custodian, written copies of the results of a threat assessment and a privacy impact assessment of the services provided;
- Ensure that any third party that provides services to the health information network provider complies with the restrictions and conditions necessary to enable compliance with the requirements of *PHIPA*; and

- Enter into a written agreement with each health information custodian concerning the services provided.

Physicians should ensure that all of their electronic service providers, including health information network providers, adhere to the requirements of *PHIPA*.

Education and Training

Since there are unique risks associated with maintaining electronic records of personal health information, physicians will have to ensure that all of their agents receive appropriate privacy and security training focussing on these risks, and polices and procedures developed and implemented to mitigate these risks, prior to being given access to the new electronic system. At a minimum, this training should cover the topics discussed in this paper.

Updating Written Information Practices

The implementation of systems of electronic records may necessitate changes to a physicians information practices. For example, physicians would have to modify the administrative, technical and physical safeguards and practices that are maintained with respect to personal health information in making the transition to electronic health records. In conjunction with the introduction of EMRs and PHRs, physicians may also provide new mechanisms for patients to access and correct records of their own personal health information. Patients can be notified of such changes through the written statement of information practices that physicians must make available to the public under *PHIPA*.

Using Electronic Patient Information

Setting Access Controls

Whether physicians are introducing an EMR or an EHR into their practices, decisions will have to made about who has access to what information, and for what purposes. In general, under *PHIPA*, health information custodians are not permitted to collect, use or disclose personal health information if other information will serve the purpose, and they are not permitted to collect, use or disclose more personal health information than is reasonably necessary to meet the purpose. Therefore, physicians should restrict access to staff on a need-to-know basis, for the purpose of carrying out their job functions.

Using Strong Passwords

Many systems of electronic health information rely on log-in passwords as the first line of defense against unauthorized access. Strong log-in passwords are usually characterized by:

- No dictionary words;
- A combination of letters, numbers and symbols;
- Eight or more characters, with 14 or more being ideal.

Since strong passwords can be difficult to remember, users are often tempted to use weak passwords. For example, the phrase "LetMeIn" may be easy to remember, but it is a weak password because it uses dictionary words. On the other hand, a system user could remember the phrase, "My birthday is October 21 and I'm 25" which becomes the password "MbiO21&i25". This would qualify as a strong password. A system favoured by the Commissioner is using the same word in two languages, such as "coat" in English and "manteau" in French, to generate the password "coatmanteau."

All staff must be made aware of the threat posed by weak passwords, especially those that are not changed frequently, and trained on how to create and protect strong passwords. In addition, the IPC recommends the use of readily available software to enforce strong password policies and to ensure that passwords are changed on a regular basis. Such software will force users to create strong passwords and change their passwords on a predetermined schedule.

It is also important to remember that even strong log-in passwords may be written down, stolen, shared, hacked, or cracked with readily available software. Thus, although 'strong' log-in passwords may prevent casual access to information, they may not prevent access by knowledgeable thieves. Therefore, strong passwords must be used in conjunction with other safeguards, such as encryption.

E-mail

Once personal health information is made available in electronic format, physicians may be tempted to transmit this information, via e-mail, to other health-care providers and their patients. E-mail is a convenient, inexpensive and quick means of communicating large quantities of electronic information. However, as a general rule, e-mail is not a secure means of communication and may be vulnerable to interception and hacking by unauthorized third parties. Unless physicians have access to a secure e-mail service offering strong encryption, they should avoid using e-mail to communicate personal health information. The e-mail service must meet PHIPA requirements; users must keep messages within the network, and save them only on secure devices.

Even if patients may be willing to accept the risk of unauthorized disclosure of their personal health information in exchange for the convenience of communicating with their physician via e-mail, this does not alleviate physicians of their duty to take steps that are reasonable in the circumstances to safeguard personal health information in their custody and control.

There are several products and services that are available now to physicians to permit them to communicate via secure e-mail. It is important to note that both the sender and the receiver must use the same secure e-mail service.

For example, eHealth Ontario offers a service referred to as ONE Mail. ONE Mail is a secure, reliable and confidential e-mail service offered to physicians who register with OntarioMD, a subsidiary of the Ontario Medical Association that receives funding from the Ministry of Health and Long-Term Care. Physicians can use ONE Mail to:

- Refer patients or receive referrals from other physicians;
- Provide other physicians with personal health information about a patient;
- Consult with other physicians;
- Avoid phoning, sending faxes, or using couriers to send personal health information to other physicians.

Using Portable Storage Devices

Once personal health information is available in electronic format, it can be easily transferred to portable storage media and transported outside of the workplace. Notwithstanding the ease of use and portability of electronic documents, it is important to note that only the minimum necessary data be transported in this manner.

Due to the high incidence of loss or theft of mobile devices such as laptop computers, personal digital assistants (PDAs), or flash drives, physicians must limit the amount of personal health information stored on portable storage media. They must also ensure that any personal health information that is stored on a mobile device is encrypted. When encryption is implemented properly, it renders personal health information safe from disclosure. The availability of encryption makes it much easier to generally safeguard electronic records of personal health information being transported than it is to safeguard paper-based records.

Encryption is a process by which ordinary text or data, referred to as *plaintext*, is turned into an unintelligible stream of seemingly random symbols, referred to as *cyphertext*. This process is controlled by a *digital key*, which will allow access to the encrypted data. The key could be:

- something you know, such as a strong password distinct from a log-in password, since there are well known methods for cracking log-in passwords; or

- something you have, such as a USB drive or token; or
- something you are, such as your fingerprint scan, retinal scan or signature.

Without the key, the data is unreadable. For example, the phrase "plain text" could be transformed to "~Sš£WÕN3@ƒ" when encrypted. The effectiveness of encryption depends on a number of factors, such as the encryption standard used, the strength of the encryption key, and the secrecy surrounding the key used.

Following the theft of a laptop computer containing the personal health information of a large number of research subjects, the IPC issued an Order (HO-004) warning health information custodians about the risks of storing personal health information on portable media. The IPC stated that in the event that a mobile device was lost or stolen, it would not be regarded as a privacy breach if sufficient safeguards were in place to ensure that personal health information was not disclosed. Therefore, properly encrypting data on portable devices could save custodians considerable time and money by allowing them to avoid the notification requirements of *PHIPA*, if the portable device was lost or stolen. It could also help prevent the potentially irreparable damage to a custodian's reputation resulting from the loss or theft of personal health information. More importantly, it would protect individuals from the undue stress of knowing that their personal health information had been lost or stolen. This is now a requirement in Ontario – health information custodians must either de-identify records of health information before transferring them to a portable device, or encrypt them. No identifiable data may be transported on a portable device, unless it is encrypted.

For information on how to encrypt information on portable devices refer to the IPC fact sheet, *Encrypting Personal Health Information on Mobile Devices*, available at www.ipc.on.ca.

Using Wireless Technology

Wireless technologies can reduce costs, increase efficiencies, and make important information more readily and widely available. For example, wireless data communications now make it possible for paramedics to send cardiac images and data directly to cardiologists, significantly reducing wait time for treatment – an excellent benefit.

Wireless devices have a number of common characteristics. The most significant is that they broadcast information over radio waves. Though they may be encoded differently (some analog, some digital), all radio waves are broadcast in all directions from the point of transmission. This means that signals may be received by any receiver within range that is tuned into the frequency of the signal. Since systems administrators are not able to identify who has accessed a wireless signal, any inadvertent disclosures of personal health information to unauthorized parties would not be detected.

In 2007, the IPC issued an Order (HO-005) after images of a patient providing a urine sample in a methadone clinic, transmitted over a wireless video monitoring system, were inadvertently

intercepted by a rear-view backup camera being used in an adjacent parking lot. The Order warned health information custodians about the threat posed by wireless technology and mandated the use of strong safeguards, such as encryption, whenever personal information is transmitted using wireless technology. Therefore, in Ontario, health information transmitted wirelessly must either be de-identified or strongly encrypted – no other option is available.

Wi-Fi

Wireless Fidelity (Wi-Fi) refers to a range of technologies for wireless data networking. Basically, wireless data networking links computers without wires. Due to their low cost, wireless routers are increasingly common in home and small office computer networks.

If the data are not encrypted or if an outdated and inadequate form of encryption is used (e.g., Wired Equivalent Privacy or WEP), personal health information transmitted over these wireless networks may be vulnerable to interception. For example, it is believed that a WEP-encrypted wireless network may have allowed thieves to steal the credit and debit card information of over 45 million T.J.Maxx customers.

The use of up-to-date transmission encryption will minimize the risk of unauthorized interception. Large organizations may wish to use virtual private networks (VPNs) for mobile workers, while individuals or smaller organizations may use Wi-Fi Protected Access (WPA or WPA2).

It is important that physicians remember that any wireless-equipped device connected to a network can serve as an illicit entry point for the *entire network* if it is not properly set up. To prevent data leakage from wireless access points, it is vital to secure the entire network end-to-end rather than just stand-alone devices.

Bluetooth®

Bluetooth® technology connects electronic devices using short-range wireless signals. It is used to link cell phones to headsets, keyboards to mice, and laptops to printers through a "pairing" process. In addition, some recent generation home monitoring systems for vital signs, weights, glucometers, and other devices utilize a mobile phone hub through Bluetooth to send data to PHRs and EMRs for chronic disease management.

Though security options are available, some of these systems are not fully secure and cases of unauthorized access have been documented. Not all devices are equally vulnerable, and manufacturers are currently making efforts to address security issues. Nonetheless, physicians should ensure that all Bluetooth® devices are appropriately secured, and that any personal health information transmitted is de-identified. Physicians should not enable Bluetooth® on any device containing or having access to personal health information without confirming that the connection is, in fact, secure and strongly protected.

Smartphones

Although definitions vary, mobile phones with advanced functionality may be regarded as a single category of wireless technology. Such devices can be used not only for voice transmission, but also as wireless modems or web browsers. When used to transmit or store personal health information, these devices can pose additional risks.

Smartphones must be configured to operate in a secure manner. Security features include the encryption of transmissions, password protection, and automated data wiping. It is also important not to use cell phones or PDAs to discuss personal or sensitive business information in public places.

As wireless communication technology becomes fully integrated into information systems and business processes, it is inevitable that substantial amounts of personal health information will flow over the airwaves. Since radio waves are a broadcast medium, capable of being received by anyone who is in range, reception of the signal by unauthorized receivers cannot be prevented. Therefore, personal health information transmitted to and from such devices must be strongly encrypted at all times.

For more information on wireless technology refer to the IPC fact sheet, *Wireless Communication Technologies: Safeguarding Privacy & Security*, available at www.ipc.on.ca.

Audit Logs

Most electronic systems of records of personal health information generate logs of transactions. By reviewing the transaction histories on a regular basis, physicians can deter and detect unauthorized access and other suspicious behaviour. In addition, the logs can be used to aid in the investigation of self-identified privacy breaches and privacy complaints that may be lodged against physicians or their employees.

Where physicians are using a network provided by a health information network provider, the provider is required under *PHIPA*, to the extent that is reasonably practical, to make available to the physician, upon request, a electronic record of:

- all accesses to the personal health information associated with the physician being held in equipment controlled by the provider, identifying the person who accessed the information, and the date and time of the access; and
- all transfers of the information associated with the physician by means of equipment controlled by the provider.

Providing Patients with Access

Under *PHIPA*, with limited exceptions, individuals have a right to access and request correction of their records of personal health information. In response to a request for access, physicians

must make the record available to the individual for examination and, at the request of the individual, provide a copy of the record to the individual. This obligation applies equally to paper-based and electronic records. To reduce the number of access requests, physicians may wish to consider providing their patients with routine access to their own personal health information through a patient portal or other PHR.

Managing Old Paper-Based Records

Once physicians have made the transition to electronic health records, they must decide what to do with their old paper-based records. Improper management of these records may not only lead to breaches of privacy, but may also deprive individuals of their right to access and correct records of personal health information. Further, to the extent that paper-based records of personal health information are not available to individuals and their health-care providers following the transition to electronic records, the continuity of care of the individuals may be put in jeopardy. Therefore, it is important that physicians manage their old paper-based records in an appropriate manner.

When physicians decide to make the transition to electronic records, they must decide whether to retain their old paper-based records, transfer them to an archive, or dispose of them. Whatever option is chosen, *PHIPA* requires physicians to ensure that records of personal health information in their custody or control are retained, transferred and disposed of in a secure manner.

Retaining Paper-Based Records

In most cases, unless the required retention period for the paper-based records has expired or the paper-based records have been duplicated in their entirety in electronic format (e.g., scanned and attached to an electronic record), physicians will need to retain their paper-based records. In terms of the legal requirements to retain records, section 13(2) of *PHIPA* only requires a custodian with custody or control of personal health information that is the subject of a request for access under section 53 of *PHIPA*, to retain the personal health information for as long as necessary to allow the individual to exhaust any recourse under *PHIPA* regarding the request. Since there are no other retention requirements in *PHIPA*, physicians should consult their governing legislation and the policies and standards of practice of the College of Physicians and Surgeons of Ontario (CPSO) in regard to the specific retention periods for records of personal health information.

According to the CPSO, physicians are required by a regulation under the *Medicine Act* to retain records for ten years from the date of the last entry in the record, for adult patients. For patients who are children, the regulation requires that the physician keep the record until ten years after the day on which the patient reached or would have reached the age of 18 years. However, the CPSO notes that it would be prudent for physicians to maintain

records for a minimum of 15 years because, in accordance with the *Limitations Act*, some legal proceedings against physicians can be brought 15 years after the act or omission on which the claim is based took place.

Until the retention period has expired, physicians may either fulfill their obligation to retain old paper-based records in a secure manner or employ the services of an agent to do so on their behalf. It is important to note, however, that a physician remains responsible for the records of personal health information, even where the records are being retained by an agent, such as a record storage company. While services may be outsourced, accountability cannot.

It is recommended that, prior to retaining paper-based records of personal health information through an agent, such as a record storage company, the physician enter into a written agreement with the agent setting out the following:

- The agent must abide by the information practices of the physician with respect to the records of personal health information that it stores on behalf of the physician;
- The agent may only collect, use, disclose, retain and dispose of personal health information on the physician's behalf if the physician permits it to do so in accordance with certain requirements. Specifically, the physician must be permitted or required to collect, use, disclose, retain or dispose of the information and the collection, use, disclosure, retention or disposition of the information must be in the course of the agent's duties and not contrary to the limits imposed by the physician or by law;
- The purpose(s) for which the agent may collect, use, disclose, retain and dispose of person health information on behalf of the physician;
- Any limits the physician imposes on the agent with respect to the collection, use, disclosure, retention, or disposal of personal health information;
- The steps that must be taken by the agent to ensure that personal health information that it stores on behalf of the physician is protected against theft, loss and unauthorized use or disclosure and to ensure that the records are protected against unauthorized copying, modification or disposal;
- The steps that must be taken by the agent to ensure that personal health information that it stores on behalf of the physician is retained, transferred and disposed of in a secure manner;
- The procedures the agent must follow to allow individuals to access and correct records of personal health information in accordance with *PHIPA*;
- The fees that the agent may charge on behalf of the physician for access to records of personal health information; and

- The agent must notify the physician at the first reasonable opportunity if personal health information handled by the agent is stolen, lost or accessed by unauthorized persons.

Disposal of Old Paper-Based Records

Physicians may securely dispose of records of personal health information when permitted to do so under *PHIPA* and after the specific retention period applicable to the records has expired or after the paper-based records have been duplicated entirely in electronic format (e.g., scanned and attached to the electronic record).

An investigation by the IPC into how health records ended up strewn across the streets of downtown Toronto determined that documents containing personal health information had not been securely handled or properly disposed of. This resulted in the IPC's first Order (HO-001) under *PHIPA*. This high-profile incident dealing with paper-based records containing personal health information highlighted the need for secure destruction practices for both paper-based records and records in other formats.

Section 1(5.1) of Regulation 329/04 under *PHIPA* defines "disposed of in a secure manner." According to this definition, when records of personal health information are destroyed, they must be destroyed in such a manner that their reconstruction is not reasonably foreseeable. Thus, the goal of record destruction is to have records containing any personal information permanently destroyed or erased in an irreversible manner that ensures that the record cannot be reconstructed in any way. Physicians should note that this applies not only to their "official" files but also to any duplicate copies of documents made for in-office use (documents could carry "shred after" dates or "do not copy" warnings).

For paper records, destruction means cross-cut shredding, not simply continuous (single strip) shredding, which can be reconstructed. Since it is technically possible to reconstruct even cross-cut shredded documents, physicians should consider pulverization or incineration of records that are highly sensitive. Physicians should consider whether on-site or off-site destruction by a licensed service provider is more suitable for their organization.

When engaging a third party service provider, physicians should look for a provider accredited by an industrial trade association, such as the National Association for Information Destruction (NAID), or willing to commit to upholding its principles, including undergoing independent audits. Physician should check references, and insist on a signed contract spelling out the terms of the relationship. The contract should:

- set out the responsibility of the service provider for the secure destruction of the records involved;
- specify how the destruction will be accomplished, under what conditions, and by whom;
- require that a certificate of destruction be issued upon completion, including the date, time, location, and method of destruction and the signature of the operator (while a

certificate itself cannot prove that destruction has actually occurred, its existence, along with the written service contract, documented reference-checking, accreditation, etc., demonstrates that you have taken reasonable steps to ensure that secure destruction has taken place);

- include a provision that would allow the physician to witness the destruction, wherever it occurs, and visit the service provider's facility;
- state that employees must be trained in and understand the importance of the secure destruction of personal health information;
- require that if any of the work is subcontracted to a third party, the service provider must notify the physician ahead of time, and have a written contractual agreement with the third party, consistent with the service provider's obligations to the physician;
- specify a time within which records collected from the physician will be destroyed, and require secure storage pending such destruction.

Transfer of Records

In rare circumstances, where the paper-based records have archival value and the required retention period has expired, the old paper-based records may be transferred to an archive in a secure manner.

Managing Privacy Breaches

Physicians' offices will be particularly vulnerable to privacy breaches during the transition from paper-based records to electronic systems of personal health information, prior to the time when medical and administrative staff members have been properly trained; access controls and other privacy features have been enabled; and old paper-based records have been stored, transferred or disposed of in a secure manner.

Privacy breaches occur whenever a person contravenes the privacy policy of an organization or a provision of *PHIPA* or its regulations, including section 12(1), which requires custodians to take steps that are reasonable in the circumstances to ensure personal health information is protected against theft, loss and unauthorized use and disclosure and to ensure that records containing personal health information are protected against unauthorized copying, modification or disposal. Most often breaches are unintentional and occur because of a lack of awareness and training. But, occasionally, breaches are intentional, such as when an employee accesses the personal health information of a known individual out of curiosity or for some other unauthorized purpose.

Because privacy breaches appear to be inevitable, physicians should have a privacy breach protocol to contain the damage by:

- Allowing staff to respond quickly and in a coordinated manner;
- Clarifying the roles and responsibilities of staff;
- Documenting the process for effective investigations;
- Allowing for effective remediation; and
- Preparing the physician for a potential investigation by the IPC.

In the paper entitled, *What to do When Faced With a Privacy Breach: Guidelines for the Health Sector*, the IPC recommends a four-step process:

- Respond immediately by implementing the privacy breach protocol;
- Containment – Identify the scope of the potential breach and take the necessary steps to contain it, as quickly as possible;
- Notification – Identify those individuals whose privacy was breached and notify them of the breach;
- Investigation and Remediation.

Physicians may be able to avoid breaches by adopting the following proactive measures:

- Educating staff about the privacy rules governing the collection, retention, use and disclosure of personal health information set out in *PHIPA*;
- Educating staff about the privacy rules governing the safe and secure disposal of personal health information and the security of records;
- Ensuring that policies and procedures are in place that comply with the privacy protection provisions of *PHIPA* and that staff are properly trained in this respect;
- Safeguarding personal health information when it is physically removed from the office or health-care facility; for example, by ensuring that all laptops and PDA's are password-protected and all data are encrypted;
- Ensuring that a baseline of logging and auditing is in place on all systems, particularly those containing electronic health records, and that staff are aware that regular audits will be conducted;
- Conducting a PIA in full, where appropriate.
- When in doubt, obtaining advice from your organization's Chief Privacy Officer and legal advisors; and
- Consulting with the IPC's Policy Department.

Resources for Physicians

There are many resources available to physicians that wish to make the transition from paper-based records to electronic health records. The Physician IT Program was developed by the ePhysician Project in collaboration with many Ontario physicians. The ePhysician Project is a partnership of the Ministry of Health and Long-Term Care, including the Ontario Family Health Network, and the Ontario Medical Association. The Physician IT Program is managed by OntarioMD, a subsidiary of the Ontario Medical Association, with funding provided by the Ontario Government. The Physician IT Program has been designed to meet the information technology needs of primary care physicians.

The Physician IT Program includes the following:

- OntarioMD.ca, an internet portal that provides access to products and services and is available to all physicians;
- Network services provided by eHealth Ontario connects all doctors in the province via a secure network;
- A selection of Clinical Management Systems (CMS) offerings that have been approved as meeting specified security, technology, and functionality standards for managing electronic medical records and practice management information;
- A Transition Support Program designed to help physicians acquire and use information technology, including access to Practice Management Consultations and workshops and tools such as best practice guidelines and checklists;
- A Primary Care IT Funding Plan designed to assist eligible primary care physicians to acquire information technology.

Recently, OntarioMD, on behalf of the Ministry of Health and Long-Term Care and the Ontario Medical Association, conducted a survey of physicians participating in the Primary Care IT Funding Program.[7] Physicians who participated in the survey reported that their use of an EMR improved health-care delivery without significantly impacting long term productivity. Improvements were noted in the following areas:

- Continuity of care (64 per cent);
- Quality of care (57 per cent);
- Patient safety (68 per cent);
- Security and privacy of patient information (40 per cent);
- Productivity (46 per cent);
- Practice revenues (34 per cent);
- Ease of recording and keeping track of patient data (64 per cent).

For further information, please contact the OntarioMD website at www.ontariomd.ca.

7 OntarioMD commissioned KPMP in partnership with the Innovative Research Group to conduct two online surveys in June and July of 2008 – one survey involved physician leads for groups of funded physicians and the other involved funded physicians.

A Word from Dr. Stephen McLaren – An EMR User for Ten Years

It has been ten years since I last saw office medical records go out of the office, on their way to a provider's home, for chart completion. It has been ten years since I have heard "I can't find the chart" begging the obvious "if it's not here, where is it?" We no longer have stacks of paper charts at reception, nursing, and in hallway carts; in health-care providers in and out baskets, homes, and cars; as well as on readily accessible filing shelves. In-house, user names and passwords protect access to the EMR; remote access requires four-factor authentication. Hardwired workstations, with no data on portable devices, simplifies security. Our Privacy Policy further enhances privacy protection and links employment to privacy compliance.

The benefits of a chartless environment via medical practice entrenched in an EMR are enormous. The ability to legibly embed detailed notes showing the story of the patient, the thoughts that went into the care, and the guidelines that influenced the decisions, all contribute to enhanced patient care and facilitate group/team care to all patients. Individual patients benefit greatly from the ability to "trend" their data. The simplest example is Prostate-Specific Antigen (PSA) test result tables showing incremental changes each year. This can lead to early diagnosis of prostate cancer, when an incremental change, greater than what was expected, is found. Such changes would not necessarily be illuminated in the paper world. Diabetics and Coronary Artery Disease patients also benefit from seeing trends in data relevant to their particular chronic disease.

Simple "flags" remind both providers and patients that their care is being "actively" managed. For example, "You have a recall set for 2015 for a colonoscopy and 2010 for Tetanus."

Population health is also facilitated by a robust EMR. Numerous clinical questions can been asked and answered accurately. For example, "How many of my patients over 65 have had pneumovax?" While the answer was 50 per cent when paper-based records were used, with the assistance of an EMR, I now know that the actual number is greater than 95 per cent. Other examples include "What medications did I prescribe for hypertensive patients in 1999 in comparison to 2006?" "Did my prescribing pattern change over time?" The answer is "yes". As expected, based on changing knowledge, I prescribed more angiotensin converting enzyme (ACE) inhibitors/angiotensin receptor blockers (ARB) and more HMG CoA, etc.

The use of an EMR also means that new practice guidelines are easier to implement. For example, in 2008, guidelines recommended all male patients, from 65 to 75 years of age, be screened using ultrasound for abdominal aortic aneurysm (AAA). I simply queried the EMR for a list of appropriate patients and sent out a one-page educational letter, along with website references and an ultrasound requisition, signed and ready to go. As a result, 90 per cent of the patients contacted were screened.

There are other benefits, such as simply being able to print out tables of trended data or actual results, or exporting components of the medical chart into an electronic file that may be shared with patients via an electronic media. This type of enhanced customer service is made possible with an EMR. In fact, supported self-management is a big winner with an EMR, something that is not easily attainable in the paper world. The next step is patient portals and direct patient access to laboratory test, allergies, prescription lists and select result data.

These are just a few of the good things. On the negative side, the sweat equity that has gone into making this work is probably the biggest downside, along with the lack of "e-deliverables" from so many who are still living in a paper world.

Summary and Conclusion

Personal health information may be at its greatest risk of exposure to privacy and security breaches when physicians are making the transition from paper-based records to electronic health records. To minimize exposure to these risks, during this period, it is important to limit the transition phase to the shortest time possible, through careful planning and preparation.

Before making the transition to electronic records of personal health information, physicians should assess the appropriateness and feasibility of conducting a PIA to determine the actual or potential threats that the new information system may have on individual's privacy and to identify ways in which these risks can be mitigated. Physicians should also ensure that they have sufficient human resources and technical expertise to implement the new technology; to enter personal health information into the new system; and to manage old paper-based records in a privacy-protective and secure manner. Staff must be educated and trained on the new system and the privacy and security risks unique to electronic records. In cases where the physician does not have the resources or technical expertise (including privacy and security expertise), to make a smooth transition to electronic records of personal health information, they should seek external support. Third party providers should be contractually bound to adhere to strict privacy and security requirements, including those set out in *PHIPA*.

Access to electronic records of personal health information should be limited to medical and administrative staff on a need-to-know basis, for the purposes of carrying out their job functions. All staff should be required to construct, use and protect strong passwords that are updated on a regular basis. The transmission of personal health information via e-mail should be prohibited, unless the information is encrypted or de-identified. The transfer of personal health information to portable storage media for transporting outside of the workplace should be avoided, unless it is limited to the absolute minimum necessary and strongly encrypted. Similarly, personal health information should not be transmitted via wireless technology, unless it is protected with safeguards, such as strong encryption. Audit logs should be maintained and reviewed regularly to deter and detect unauthorized access and other suspicious behaviour. Policies and procedures for providing patients access to their own electronic records of personal health information requires further development and implementation.

Once the transition to electronic records of personal health information has been made, physicians need to retain, transfer or dispose of old paper-based records of personal health information in a secure manner. Old paper-based records should not be destroyed unless permitted by *PHIPA*, and the required retention period applicable to the record has expired or the entire paper-based record has been duplicated in electronic format.

Finally, because privacy breaches appear to be inevitable, physicians should ensure that they have a privacy breach protocol in place to manage any breaches that may occur.

Although electronic systems pose a new set of challenges for the protection of personal health information, these challenges can be effectively addressed with existing technologies and processes. With careful consideration of the risks highlighted in this toolkit, electronic records of personal health information can be designed and implemented in manner that enhances privacy. Physicians that have made the transition to electronic health records resoundingly agree that the benefits to patient care make it well worth the effort.

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

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