BC Physician Privacy Toolkit

2nd edition – June 15th, 2009

WARNING AND DISCLAIMER

This BC Physician Privacy Toolkit has been prepared by the BC Medical Association (BCMA), the College of Physicians and Surgeons of BC (College) and the Office of the Information and Privacy Commissioner for BC (OIPC), as a general guide to assist physicians to meet their obligations under the Personal Information Protection Act (PIPA).

- This Toolkit is designed to assist in complying with the law and meeting the changing expectations of patients and the public. It reflects interpretations and practices regarded as valid when it was published based on available information at that time.

- The resource materials provided in this Toolkit are for general information purposes only. They should be adapted to the circumstances of each physician using the Toolkit.

- This toolkit does not fetter or bind, or constitute a decision or finding by the BCMA, the College or the OIPC and is not intended, and should not be construed, as legal or professional advice or opinion. Physicians concerned about the applicability of privacy legislation to their activities are advised to seek legal or professional advice based on their particular circumstances.

INVITATION FOR FEEDBACK

This is the second edition of the BC Physician Privacy Toolkit. Your feedback is always appreciated. Please contact any of the three organisations with your questions or comments:

- BC Medical Association (BCMA) - www.bcma.org

- College of Physicians and Surgeons of BC (College) www.cpsbc.ca

- Office of the Information and Privacy Commissioner for BC (OIPC) www.oipc.bc.ca

Table of contents

Privacy and Security in the BC Health Care System Today

This section will:

- Summarize the privacy legislation in BC that applies to physicians in private practice (PIPA) and the requirements related to patient consent.
- Summarize the privacy legislation in BC that applies to health care organizations and government (FIPPA and e-Health Act).
- Explain the difference between PIPA and FIPPA.
- Explain the role of the BC Information and Privacy Commissioner.
- Identify key elements of physician compliance with data stewardship requirements.
- Introduce key notions on data stewardship (paper and electronic) for physicians relating to both information in their practice and information shared outside their practice.
- Explain the difference between Electronic Medical Records (EMRs) and Electronic Health Records (EHRs).

Privacy and Security in the BC Health Care System Today

Health information is one of the most sensitive forms of personal information. Health information is used for a number of purposes, including patient care, financial reimbursement, medical education, research, social services, quality assurance, risk management, public health regulation, litigation, and commercial concerns.

Both privacy and security of personal health information are major concerns for physicians because both are fundamental to the confidentiality and trust of the physician-patient relationship. If patients do not have the confidence that their privacy will be maintained, or that reasonable security safeguards will be in place to protect their information, they may do things to protect their privacy on their own (such as refrain from disclosing critical information, refuse to provide consent to use personal health information for research purposes, or not seek treatment). Such behavior was illustrated in a 1999 Canadian Medical Association (CMA) survey, which found that 11% of the public held back information from a health care provider due to concerns about whom it would be shared with or what purposes it would be used for.

Patients are also concerned about wrongful release of information to third parties, which may result in harm to the patients. The Supreme Court of Canada has recognized that Section 7 of the Canadian Charter of Rights and Freedoms includes the right to be free of the psychological stress resulting from the unauthorized disclosure of one's personal health information.

Physicians are governed by the professional requirements in the CMA Code of Ethics (see cma.ca) and the regulatory standards in the College of Physicians and Surgeons of BC Data Stewardship Principles (see www.cpsbc.ca). In addition, for private practice physicians, including their employees and staff, obligations concerning the privacy of information are enforced by the Personal Information Protection Act (PIPA) (see below). This BC Physician Privacy Toolkit focuses on physicians' responsibilities under PIPA.

For physicians who operate within public health care organizations, such as hospitals, Health Authorities, and the health ministries, the applicable privacy protection measures are contained in the Freedom of Information and Protection of Privacy Act (FIPPA or FOIPPA; see below).

Privacy and security in the health care system today must balance two competing social benefits: the need to appropriately access and share information to enhance care quality and safety and provide continuity of care, and the need to implement reasonable safeguards to maintain the privacy of personal health information. Balancing these two needs presents a challenge, one that can be met through a variety of measures ranging from administrative and personnel security safeguards (e.g., employee training, policies, confidentiality agreements) to technical solutions (e.g., roles-based access control, auditing, authentication mechanisms, encryption). Implementing these factors will build and maintain public trust in the privacy and security of personal health information.

Adequately protecting personal health information is a complex process within the context of a patchwork of privacy legislation, new information technologies (including Electronic Medical Records (EMRs) and Electronic Health Records (EHRs)), new models for information sharing, collaborative teams, partnerships, and mergers. But none of these factors, including the introduction of new information technologies, change the responsibilities of physicians to appropriately protect patient information; nor do they eliminate the risks to patient information. Rather, different methods for safeguarding personal information that is stored electronically must be considered and implemented. (Note that industry experience has shown that while the threat of hackers is viewed as a major security threat to electronic systems, most instances of privacy and security breaches occur within organizations by staff who have legitimate access.)

BC's Personal Information Protection Act (PIPA)

The Personal Information Protection Act (PIPA) applies to private physicians' offices and governs how personal health information of patients, employees, and volunteers may be collected, used, and disclosed.

PIPA came into force on January 1st, 2004, to govern the BC private sector—both for-profit and not-for-profit. Any organization to which PIPA applies is exempted from the federal legislation, the Personal Information Protection and Electronic Documents Act (PIPEDA), which applies only to a "federal work, undertaking, or business" as defined in Section 1 of that Act.

PIPA **does not** apply to personal information collected and stored by public health care organizations such as hospitals, Health Authorities, and the health ministries. Those entities are instead governed by the Freedom of Information and Protection of Privacy Act (FIPPA, see below). As well, PIPA **does not** apply to information to which FIPPA applies or information in the custody or control of a federal undertaking, to which the federal private sector privacy legislation (PIPEDA—Personal Information Protection and Electronic Documents Act) applies.

PIPA applies to personal information. In this context, "personal information" means both information that can identify an individual (e.g., name, home address, home phone number, ID numbers), and information about an identifiable individual (e.g., physical description, educational qualifications, blood type). As well, personal information includes employee personal information, but **not** business contact information, work product information, or anonymous/aggregate information.

The core principle of PIPA that is relevant to physicians is that personal information should not be collected, used, or disclosed without the prior knowledge and consent of the patient, which may be implicit. This principle is subject to limited exceptions. For example:

- Where the collection, use, and/or disclosure is clearly in the interests of the individual and consent cannot be obtained in a timely way.
- Where the collection, use, and/or disclosure is necessary for medical treatment of the individual and the individual is either unable to give consent or does not have the legal capacity to give consent.

Under PIPA, the consent for collection, use, and disclosure of personal information for direct health care purposes in BC operates primarily on an "implied consent" model. This means that those individuals who form part of a patient's "circle of care" (e.g., specialists, referring physicians, lab technologists) can access, use, disclose, and retain patient information for the purposes of ongoing care and treatment.

However, implied consent must be informed, and physicians should provide adequate information to patients on how they manage the privacy of patient information (see the section, Ten Steps to Help Physicians Comply with PIPA, and the handout Privacy of Your Personal Health Information). Implied consent is signified by a reasonable individual accepting the collection, use, and disclosure of information for an obvious purpose where it is understood that the individual will indicate if he or she does not accept

(the “opt-out” model). For implied consent to be meaningful, the individual has to know that he or she has the right to expressly withhold or withdraw consent at any time without fear of retribution.

Expressed consent from a patient is required when identifiable personal information is intended to be collected, used, or disclosed outside of the circle of care, or for secondary purposes such as research (see the section Secondary Use of Personal Information for Research). Expressed consent is signified by the individual willingly agreeing to the collection, use, and disclosure of personal information for a defined purpose (the “opt-in” model). The consent can be given verbally or in writing.

Under PIPA, physicians have custody of the personal health information that they have collected and physical ownership of the documents/electronic data. They are accountable for any privacy breach that occurs to patient information in their custody and control, including any breach committed by an employee under their authority. The individual patient has the right to control, with limited exceptions under Section 18 of the Act, the collection, use, and disclosure of that data.

BC’s Freedom of Information and Protection of Privacy Act (FIPPA)

In BC, public health care organizations such as hospitals, Health Authorities, and the health ministries are subject to the privacy protection measures contained in the Freedom of Information and Protection of Privacy Act (FIPPA, also referred to as FOIPPA). FIPPA guarantees the right of the public to gain access to and request correction of personal information collected about them by public bodies and prevents the unauthorized collection, use, or disclosure of personal information by public bodies. It also requires that reasonable safeguards be in place to protect personal information. FIPPA **does not** apply to personal information collected and stored by private physician offices, private laboratories, or other private health providers. The BC Personal Information Protection Act (PIPA, see above) governs these entities.

An amendment to FIPPA, Bill 73, was brought into effect in 2004 and prohibits the disclosure of personal identifiable information outside of Canada as well as any access to such records from outside Canada without explicit consent (except in limited circumstances). Under whistle-blower protection, individuals are expected to report unauthorized disclosure and access as well as foreign demand for disclosure or access.

Bill 30, which was introduced in 2006, amends some aspects of Bill 73. It permits "foreign access" under certain circumstances, such as out-of-country system and equipment maintenance and data recovery, but only under strict conditions. The out-of-country access must be necessary and the information can only be accessed and stored outside of Canada for the minimum amount of time to complete the task. It must also be under tightly controlled and secure circumstances.

Comparing PIPA and FIPPA

There are some notable differences between PIPA and FIPPA:

- PIPA does not include the FIPPA provisions regarding storage and access to personal information from outside Canada. As long as privacy is contractually protected, it does not matter where the data is or where it is accessed from.
- PIPA excludes business contact information from the definition of personal information.
- PIPA requires consent for the collection, use, and disclosure of personal information. It is up to the organization to determine whether the form of consent is expressed (written or verbal) or deemed (implied).
- FIPPA does not contain consent requirements; instead it operates on the principle of "notification" for collection of information.

BC's e-Health Act

The BC e-Health Act (Personal Health Information Access and Protection of Privacy Act) received Royal Assent on May 29, 2008. It was introduced to provide legislative authority and a privacy framework to protect personal health information collected in designated Health Information Banks (HIBs) by public bodies such as the Ministry of Health Services or BC Health Authorities. HIBs are the underlying data repositories that will support information access and sharing in the provincial Electronic Health Record (EHR). The e-Health Act does not override FIPPA, but supplements its provisions with the following new regulations:

- Allows individuals to issue disclosure directives to block access to (or "mask") some or all of their personal information stored in HIBs.
- Prohibits disclosure of information from an HIB for market research.
- Establishes a Data Stewardship Committee (DSC) made up of members from the health authorities, health professions including the BCMA and College of Physicians and Surgeons, and the public to evaluate requests for secondary access of information in the EHR.
- Permits patient contact information to be disclosed for the purposes of asking individuals to participate in health research, but only with the specific approval of the BC Information and Privacy Commissioner.
- Adds new whistle-blower protection to protect individuals who report privacy breaches to the chief data steward or the privacy commissioner and to encourage good faith reporting to enhance privacy protection.

- Establishes penalties for privacy and security breaches in the EHR. The penalty for privacy breaches in HIBs is a fine of up to $200,000.

Role of the BC Information and Privacy Commissioner

Monitoring compliance with BC privacy legislation (FIPPA, PIPA) is the responsibility of the provincial Information and Privacy Commissioner, who is an independent officer of the BC Legislature.

If patients have concerns related to privacy and security of their information, they can contact the Office of the Information and Privacy Commissioner (OIPC) of British Columbia at www.oipc.bc.ca. Also, if patients are unsatisfied with how their privacy complaint was addressed by the physician's practice and by the BC College of Physicians and Surgeons, they can escalate their complaint to the OIPC.

More information on the role of the Information and Privacy Commissioner for BC and privacy legislation in BC can be found at www.oipc.bc.ca.

Data Stewardship and Physician Compliance

As the traditional practice environment evolves, physicians should regularly evaluate and update their practice's data stewardship framework and related policies on accountability, information management, and privacy. This includes, but is not limited to, the following:

- Reviewing and revising policies, processes, and procedures related to the collection, use, and disclosure of personal health information within the practice and with associated health care professionals.
- Reassessing regularly if information collected is truly required and what the minimum requirement is to satisfy the intended uses.
- Managing all aspects of patient information including orders, results, reports, and managing referrals and consultations.
- Appropriately using information accessed from external electronic health records or systems and determining what should be recorded in the physician medical record.
- Ensuring that contractual agreements with appropriate privacy provisions are in place with service providers engaged to implement and support the EMR or EHR.
- Ensuring that any submission of personal information to a third party is done:
    - With respect to requirements of patient consent and privacy legislation and under an information-sharing agreement (ISA) whenever appropriate.

- With an understanding of the intended uses of the data prior to submission of such data and what controls are in place to control access (e.g., roles- and needs-based access model).
- After examination of whether it is truly required and what the minimum requirement is to satisfy the intended uses.
- With a secure protocol for data transfer including encryption whenever possible.
- With assurance that the other party has acceptable privacy and security policies and practices in place.

Individuals own their personal health information, and physicians act as data stewards, which means that physicians are responsible and accountable for the personal information they collect, use, and disclose. This responsibility is enforced through specific obligations under the BC Personal Information Protection Act (PIPA).

The College of Physicians and Surgeons of BC with representation from the BC Medical Association created a Data Stewardship Framework in May 2007 to describe how physicians can meet the requirement to protect the integrity of a patient's medical information in both the paper and electronic contexts. The BC Physician Data Stewardship Framework can be accessed from the College website (www.cpsbc.ca).

Data Stewardship within a Physician Practice: Paper Records and Electronic Medical Record (EMRs)

The traditional provider-centric model of data stewardship is one where a physician practising in a clinic environment maintains a medical record of care provided to an individual patient. That medical record can be in paper or electronic form, but the principles of physicians' data stewardship remain the same.

The Electronic Medical Record (EMR) generally refers to an electronic version of the traditional paper-based patient record used within a medical practice setting. The EMR is a comprehensive record of health information compiled during a direct patient-provider relationship and is under the stewardship of the physician providing primary care.

The physician manages the relationship with the patient as well as with others involved in the patient's circle of care. Within the practice setting, the physician is responsible for complying with applicable legislation governing personal information in addition to the professional and ethical duties in maintaining the confidentiality of patient information. This includes obtaining appropriate consent; managing the practice for collection, use, and disclosure of patient information; allowing patients access to their own personal information; correcting personal information; and securely retaining personal information. For

information on how to implement these requirements, see the section Ten Steps to Help Physicians Comply with PIPA.

Data Stewardship and Information Sharing outside of a Physician Practice: Collaborative Care and Electronic Health Records (EHRs)

Many current trends are transforming the traditional model of trust between physicians and other health professions in the sharing of information for continuity and quality of care. These include collaborative care teams, integrated health networks, and the shift to Electronic Health Records (EHRs).

Canada Health Infoway defines an Electronic Health Record as "a secure and private lifetime record of an individual's health and care history, available electronically to authorized health care providers." The EHR is generally a compilation of core data from multiple and diverse sources submitted by different providers and health care organizations, and potentially from different jurisdictions. The EMR can be a source of core data that may be automatically shared or uploaded to an EHR. The objective of an EHR is to provide authorized health care providers with timely access to relevant portions of a patient's electronic record when they need it to provide care, regardless of where a patient presents. The EHR can also allow patients access to their own records on-line.

In BC there are new and evolving models for where and how physicians work, such as primary care networks, integrated health networks, specialty-related medical groups working in association, and medical practices geographically located within Health Authority regions. With such new forms of practice and with institutional or provincial EHRs, the sharing of personal information is now broadened beyond what is customarily understood by a patient to be included in their circle of care. In patient-centric institutional or provincial EHRs, information from a broad range of sources and providers can be shared with and accessed by others. Adding further complexity is the potential for secondary uses of electronic health information by persons or organizations beyond the circle of care.

With varying levels of information-sharing, models for patient consent will vary depending on the situation, and it is not possible to establish guidelines that fit all scenarios. The interplay between physician offices governed under PIPA and public organizations governed under FIPPA is complex, and provincial collaboration is underway to define appropriate information-sharing that also meets the requirements of both pieces of legislation. Combinations of several tools (such as obtaining consent, roles- and need-based access, opt out, masking, disclosure directives, and auditing) are being used or implemented to best meet the needs of protecting patients' confidentiality and rights while sharing information appropriately and efficiently.

Establishing robust roles-based access is possible particularly in the information technology environment. The objective of a roles-based access model is to identify all possible roles that require access to patient health information, to which a standard set of patient information (e.g., lab results, medication information, registration information) and permissions (e.g., reading, writing, printing) can be assigned. Defining this model also allows for ease of account management when setting up new users and modifying accounts. Roles-based access models must be designed to support both business and clinical workflow and, therefore, the software must have the flexibility to support the unique needs of each provider. It must also allow for exceptions to the standard roles and permissions as long as they are authorized and necessary for the performance of job duties. (See the section Electronic Medical Records and Roles-Based Access.)

Roles-based access has great potential to strengthen the trust of patients by ensuring appropriate access to the patient record. However, roles-based access needs also to integrate a "need to know" principle, based on a legitimate relationship with the patient. Unfortunately, "need to know" often becomes "want to know", so it is necessary to always consider the degree to which access to the personal information is truly needed to perform a given role's duties.

Physicians as primary custodians must maintain the responsibility for stewardship of patient information that they collect, use, and disclose. While technology is changing and influencing the future of health care, data stewardship remains a professional responsibility and not a technology issue.[1] If asked to transfer information to a public health organization or to government, physicians must consider all those issues identified above in the section Data Stewardship and Physician Compliance.

EMRs vs. EHRs: What is the Difference?

The terms EMR and EHR are often used interchangeably, although an understanding of the distinctions between the two has improved as a result of a number of eHealth related initiatives in progress within BC and across Canada.

Both systems offer considerable opportunities for improving patient care, safety, and health outcomes, and both can assist health care planners in finding ways to improve on efficiencies and cost-savings. While numerous benefits are evident in EMRs and EHRs, both present similar challenges in terms of meeting the expectations of patients and protecting personal information privacy. Understandably, with the consolidation of patient information available electronically and the potential for access to that information by unauthorized persons, there are specific privacy considerations related to the following topics (each cross-referenced to various sections within this Toolkit):

[1] Data Stewardship Framework, Committee on Privacy and Data Stewardship, BC College of Physicians and Surgeons, July 31, 2007.

- Data stewardship and accountability (see the section Privacy and Security in the BC Health Care System Today).
- Consent for collection, use, and disclosure of personal information (see the section Consent and Disclosure Directives in BC).
- Secondary use for research (see the section Secondary Use of Personal Information for Research).
- Privacy and security of EMRs (see the section Privacy and Security Considerations for EMR Implementation).
- Appropriate access (see the section Electronic Medical Records and Roles-Based Access).
- Accuracy of personal information (see the section Guidelines for Ensuring Accuracy of Patient Records).
- Safeguarding personal information (see the section Protecting Patient Information in and outside of the Office).

The provincial EHR has not yet been implemented. It is anticipated that implementation will be incremental and staged over several years. However, within the various health authorities, EHRs have been implemented to varying levels. The governance of those EHRs rests with the Health Authorities regulated under FIPPA.

Currently, the policies on confidentiality of data contained within EMRs in private physicians' offices (regulated under PIPA), and particularly those policies impacting disclosure (i.e., the core data set and its components, disclosure directives, roles-based access, audit, breach policies, secondary use), have not been determined, and the implementation of the provincial EHR is conditional on those determinations, at least to the extent that implementation is to include private physicians' offices. Until that time, data from private physicians' EMRs can only be sent to consultants who share in a particular patient's care, to the extent that the data is relevant and under the implicit consent of the patient (by his or her agreement to the referral). In all other circumstances, explicit patient consent is required to disclose personal health information from the EMR.

These same constraints apply to any consortium of EMRs (e.g., community of practice initiatives), with the caveat that alternative processes (to those enabling the provincial EHR) may ultimately be engaged to enable limited data exchange and, potentially, data sharing. One way to determine whether or not there are privacy issues related to a new information exchange, whether paper or electronic or both, is to evaluate the proposed exchange using a Privacy Impact Assessment (PIA). The PIA can then help determine whether any changes are required, including possibly the need to design and implement an information sharing agreement (ISA).

Ten Principles for Protecting Patient Information in Physician Practices

This section will:
• Put into context the 10 principles that form the basis of the privacy legislation in BC to physicians in office-based practice.

The following principles are based on 10 principles of the Personal Information Protection Act (PIPA) and other privacy legislation around the world. This section provides general background and guidance, and does not replace BC's applicable privacy legislation.

Principle 1: Accountability

Physicians' offices are responsible for the personal information under their control. A Privacy Officer must be designated as being responsible for the practice's compliance with PIPA, and it is recommended that this person be a physician. This means that if the office is a solo practice, the solo physician is the *de facto* Privacy Officer. In a group practice, one of the physicians must be identified as having responsibility for this function.

Key functions of the Privacy Officer include developing and implementing policies and procedures to protect personal information; educating employees about privacy and security; ensuring that confidentiality agreements are signed; responding to inquiries, complaints, and privacy breaches; responding to patient requests for access; and overseeing the offices' privacy compliance. The Privacy Officer and the physician delegating him or her are accountable to the BC College of Physicians and Surgeons and the Office of the Information and Privacy Commissioner for BC (OIPC). (See the section Ten Steps to Help Physicians Comply with PIPA.)

Principle 2: Identifying purpose

Before collecting someone's personal information, physicians' offices should advise the patient why they are collecting it and how it will be used. Each practice should therefore assess its existing information collection practices to define and document purposes for which personal health information is collected. Most often that implicit consent would be for the purpose of collecting, using, and disclosing only that information reasonably required in the interest of the patient's own health care with the exception of caveats contained in Section 18 of PIPA

(www.oipc.bc.ca/legislation/PIPA/Personal_Information_Protection_Act.htm). If it is not possible to identify the purpose, the practice should stop collecting the data.

Principle 3: Consent

The core principle of PIPA is that personal information should not be collected, used, or disclosed without the prior knowledge and consent of the patient, subject to limited exceptions (such as certain communicable diseases or potential harm to others). Consent may be implied or expressly given; it may be given either verbally or in writing. Expressed consent is not a requirement under PIPA for direct patient care purposes or other consistent purposes, and implied consent is the norm for continuity of care. However, implied consent must be "informed and knowledgeable," and physician practices must communicate the ways in which they respect the privacy of patients and how personal information is safeguarded.

It must also be made clear to patients that there will be no retribution if they choose not to consent. (See the sample template Our Privacy Policy—Handout for Patients.)

Principle 4: Limiting collection

Physicians' offices should collect only the minimum personal information necessary to fulfill stated purposes. Information must be collected by fair and lawful means.

Principle 5: Limiting use, disclosure, and retention

Physicians' offices must use and disclose personal information in accordance with the purposes given to the patient. New uses and disclosures require new consent. Information should be kept only for as long as necessary to meet the original purposes, or as required by the policies of the College of Physicians and Surgeons of BC. Information (whether paper or electronic) should be disposed of appropriately, safely, and definitively. (See the section Secure Destruction of Personal Information.)

While PIPA does not include the FIPPA provisions regarding prohibition of storage and access to personal information from outside Canada, it is recommended that physicians avoid disclosing personal identifiable information outside of Canada and prohibit access to such records from outside Canada without expressed patient consent.

Principle 6: Accuracy

Patient information must be kept accurate, up-to-date, and as complete as necessary to fulfill stated purposes. (See the section Guidelines for Ensuring the Accuracy of Patient Records.)

Principle 7: Safeguards

Physicians' offices must implement reasonable safeguards to protect personal information against risks such as loss, theft, unauthorized access and disclosure, copying, use, or alteration. Safeguards refer to a combination of policies, processes, practices, and technologies intended to protect personal information. Safeguards appropriate to the sensitivity of the information are to be used, irrespective of the form in which patient information is stored (paper, electronic, digital, or otherwise). (See the section Protecting Patient Information inside and outside of the Office.)

Principle 8: Openness

Physicians' offices should inform patients about the personal information they collect and store, the purposes for which it is used, the persons to whom it is disclosed, and how an individual may access it. This can be achieved through patient handouts or posters. (See Our Privacy Policy—Handout for Patients.)

Principle 9: Individual access

Patients are entitled to access their personal information to ensure its accuracy and completeness, and to identify to whom it was disclosed, subject to certain exceptions. Physicians' offices may charge a minimal fee for such access. (See the section Guidelines for Responding to Patient Requests to Access Personal Information and the sample Patient Request for Access to Personal Information.)

Principle 10: Challenging compliance

Patients can challenge a practice's compliance with these principles through the practice's complaints process. They can also make a complaint to the BC College of Physicians and Surgeons at www.cpsbc.ca.

If a patient is not satisfied with the results of a response to a complaint, he or she may take the complaint to the Office of the Information and Privacy Commissioner for BC (OIPC) at www.oipc.bc.ca.

Ten Steps to Help Physicians Comply with PIPA

This section will:
• Identify the 10 essential steps that physicians in an office-based practice need to take in order to comply with PIPA.

Getting started is simple. Consider the following 10 steps to support compliance with the requirements under PIPA.

Step 1: Put someone in charge

Physicians' offices are responsible for the personal information under their control. Every medical practice must have a designated Privacy Officer accountable for helping patients understand how personal information is being managed and to be responsible for ensuring overall compliance with the Personal Information Protection Act (PIPA).

It is recommended that the Privacy Officer be a physician. This means that if the office is a solo practice, the solo physician is the *de facto* Privacy Officer. In a group practice, one of the physicians must be identified as having responsibility for this function.

The Privacy Officer must understand the following issues:

1. What kind of information is covered under PIPA.
2. What information is appropriate to collect from patients.
3. What circumstances information can be disclosed and to whom.
4. When consent from the patient is required and when it is not.
5. How patients can access their own records.
6. How patients can request corrections to their records.
7. What fees can be charged for access.
8. How to handle a privacy breach.
9. How to respond to privacy complaints.
10. What reasonable safeguards must be implemented commensurate with the level of risks to privacy.

The Privacy Officer is responsible for the practice's privacy policy (see Step 6 below) and for ensuring that procedures are fully implemented and working effectively. Key functions of the Privacy Officer include the following:

1. Developing and implementing policies and procedures to protect personal information.
2. Educating employees about privacy and security.
3. Ensuring that confidentiality agreements are signed.
4. Answering patients' questions about PIPA.
5. Responding to inquiries, complaints, and privacy breaches.
6. Responding to patients' requests for access.
7. Overseeing the office's privacy compliance.

The Privacy Officer and the physician delegating him or her are accountable to the BC College of Physicians and Surgeons and the Office of the Information and Privacy Commissioner for BC (OIPC) .

Step 2: Become familiar with PIPA's privacy principles

The Privacy Officer, physicians, and employees of the practice must familiarize themselves with PIPA's privacy principles. (See the section Ten Principles for Protecting Information in Physician Practices.)

Step 3: Review how the practice handles personal information

The first question to ask is, "What personal information does the practice collect and how does the practice currently manage it?" After that information has been gathered, these steps should be followed:

- Taking an inventory of the personal information the practice currently has.
- Identifying the information needs of the different functions within the practice.
- Identifying the current information practices (including why the practice collects, uses, and discloses personal information).

Step 4: Put information-handling practices to the test

Consider whether the information-handling practices meet PIPA obligations. If well-established ethical and professional principles are currently being applied to the management of patient information, it is unlikely that significant changes are needed. Develop a plan to overcome any deficiencies, starting with the most problematic areas. These include how to handle the most sensitive personal information collected or of the information most vulnerable to improper use or disclosure.

Step 5: Implement changes

After assessing the information-handling practices, changes may need to be made to practices and systems (technological and otherwise). Regardless of the size of the practice, any person who collects, uses, or discloses personal information should be involved in the implementation of the privacy program and security plans. Complying with the privacy principles may require a change to some computer systems or how the practice physically stores information.

Step 6: Develop a privacy policy

PIPA requires physician practices to prepare and follow a privacy policy, which must also be available for patients and employees. Security measures must also be considered when developing and implementing a privacy policy. Staff who handle personal information in the medical practice should be consulted when developing the privacy policy, and the following considerations should be incorporated into it:

1. How information will be safeguarded by physical, technological, and organizational security measures.
2. How the practice will ensure that personal information is collected accurately, stored securely, and disposed of properly.
3. How patients will be notified of why the information is being collected.
4. How patients may request access or correction to their information.
5. How the privacy of employees' personal information will be maintained.

The CMA Privacy Wizard (www.cma.ca/privacywizard.htm) was designed in collaboration with the BCMA to allow physicians to create an office privacy policy in usually under 20 minutes while earning CME credits. This privacy policy would, when posted in the office or distributed as a pamphlet, explain to patients why personal information is being collected; how it will be used, disclosed, and protected; and what their rights are. It will also provide staff, locum physicians, and physicians-in-training with clear responsibilities and expectations.

Step 7: Ensure compliance of staff and third parties

It is the staff, who will be responsible for complying with the policies on a patient-by-patient, day-to-day basis, and they must be aware of their obligations and expectations. A comprehensive privacy program should include educating staff about privacy policies and procedures. Remember: staff education is essential to success.

The practice is also responsible for ensuring that third parties (e.g., associates, locums, visiting specialists, physicians-in-training, contractors, volunteers, partners, or agents with whom the practice collects, uses, or discloses personal information) know the privacy policies, and if appropriate, sign a

confidentiality agreement. (See the sample Confidentiality Agreement for Employees of a Physician Office and the Confidentiality Agreement for Third Parties.)

Step 8: Develop and revise forms and communications materials

Review and revise forms, brochures, handouts, website content, and any other communication material to comply with PIPA, and inform patients about the office's privacy policy and information practices. A patient's implied consent to collect, use, and disclose personal information for medical treatment and continuity of care can be relied on, but it is recommended that notice of this policy be given to patients at the time the information is collected. (See the sample patient handout Our Privacy Policy that can be generated by using the CMA Privacy Wizard.)

Step 9: Review and revise contracts

The medical practice is responsible for personal information in its custody as well as under its control. This includes personal information that has been transferred for processing to a lab, for example, or information that a third party may have collected on the practice's behalf. To ensure that this personal information is properly protected, contracts should clearly require third parties to comply with PIPA and any policies that have been developed to properly manage personal information. Contracts should specify the purpose for which the third party is allowed to use the personal information and prohibit any other use or disclosure. (See the Confidentiality Agreement for Third Parties.)

Step 10: Develop an effective complaints handling process

PIPA requires that a process for handling privacy complaints be created. It is always more efficient to resolve complaints through the Privacy Officer than to involve an outside regulator (e.g., the College of Physicians and Surgeons of BC, and, failing a successful resolution, the Office of the Information and Privacy Commissioner for BC (OIPC)). Having an effective complaints-handling process is an important part of managing privacy risks within a practice.

Protecting Patient Information in and outside of the Office

This section will:
• Define safeguards for protecting patient records. • Identify best practices for protecting paper and electronic records. • Describe reasonable practices for protecting personal information outside of the office.

Safeguards are a combination of policies, processes, practices, and technologies that are intended to protect personal information. Regardless of how personal health information is recorded—whether on paper or electronically—appropriate and reasonable safeguards are necessary to ensure that privacy is protected and confidentiality is maintained.

Physicians have an ethical obligation to respect patient confidentiality, and the CMA Code of Ethics requires physicians to protect the personal health information of their patients. The Personal Information Protection Act (PIPA), requires physicians to take reasonable measures to protect patients' personal information from risks of unauthorized access, use, disclosure and disposal, and sets out the consequences for violation. In a report published in 2006, the Information and Privacy Commissioner for BC described reasonableness as "the measure by which security measures are objectively diligent and prudent in the circumstance" and stated that "what is 'reasonable' may signify a very high level of rigour depending on the situation."

Protecting Records in the Office

Patient records must be handled in a secure manner from the time the records are created to the time they are disposed of, regardless of the format upon which the information is stored.

The following guidelines should be considered and incorporated into the implementation plans for safeguarding patient records and any other personal information stored in the practice. Note that a combination of measures may be required during the transition from paper-based patient records to Electronic Medical Records (EMRs) where both methods of record-keeping may be maintained in parallel.

Staff[2] working in physician practices should:

[2] Staff include locum physicians, associates, visiting specialists, physicians-in-training, contractors, volunteers, and residents with whom you collect, use, or disclose personal information.

1. Lock doors and cabinets where patient records are stored.
2. Wear building passes/photo ID if issued.
3. Query the status of strangers.
4. Know whom to inform if suspicious behaviors are noticed
5. Not tell unauthorized individuals how security systems operate.
6. Sign confidentiality agreements that specify obligations and expectations including repercussions for inappropriately collecting, using, or disclosing personal information.

Paper records should be:

1. Formally booked out from the normal filing system.
2. Tracked, if transferred, by confirming that the records arrived at their specified destination.
3. Returned to the filing location as soon as possible after use.
4. Stored securely within the clinic or office.
5. Placed in a location where members of the public cannot view the contents.
6. Not left unattended at fax machines or photocopiers.
7. Held in secure storage with clear labelling.
8. Kept on-site wherever possible. If the records must be taken off-site, they must be kept secure at all times.

With Electronic Medical Records (EMRs), staff should:

1. Log out of computer systems or applications when not in use or unattended.
2. Keep workstations positioned away from public view and access.
3. Not share an assigned user ID and password with others. If other staff members need to access the EMR, authorized access should be granted.
4. Not write down passwords.
5. Revoke user IDs and passwords as soon as authorized users resign or are dismissed.
6. Install firewall software where Internet access to computer systems exists.
7. Ensure that data backup methods and disaster recovery plans are in place and periodically reviewed.

EMRs should provide:

1. A unique user ID and password for every authorized user.
2. Access to patient information on a “need to know” basis under a roles-based access model that determines whether the user has the necessary authorization and permissions.

3. Audit trails to track when a patient record is accessed, by whom, including date and time.
4. Enforced password changes at regular intervals.
5. Ability to easily manage user accounts (create, modify, revoke).
6. Password protected screensaver or auto log out after a period of inactivity to avoid unauthorized viewing.

Protecting Personal Information outside the Office

There are times when physicians and their staff may need to work with personal information while travelling, at home, or at another location. This includes transporting records by car or airplane, working from home, attending meetings or conferences, or making visits to a patient's or a client's home. The personal information may be stored in paper records or on portable electronic devices (such as laptops, CDs, DVDs, external hard drives, USB storage devices, handheld electronic devices and smart phones); however with the movement toward Electronic Medical Records (EMRs) and other forms of electronic communication, physicians and their staff are also able to connect to their office network, and therefore may have access to sensitive personal health information from anywhere in the world.

Under the BC Personal Information Protection Act (PIPA), physicians must implement reasonable safeguards to reduce the risks associated with working with personal information remotely while travelling, at home, or at another location.

Guidelines for conversations outside the office:

1. Avoid discussing personal information in public areas such as on elevators, in stairwells, while travelling by public transit or airplanes, in restaurants, or on the street.
2. When in transit, avoid using cell phones to discuss personal information, as these conversations can be intercepted or overheard.
3. If a staff member works regularly from home, a dedicated phone line with password protected voicemail is recommended.

Guidelines for personal information stored on paper or portable electronic devices when outside the office:

1. Remove records containing personal information only when it is absolutely necessary for performing job duties. If possible, leave a copy with the originals left in the office. Take only the minimum amount of personal information required.
2. Require all staff to obtain approval from their supervisor before removing records containing personal information from the office.

3. When travelling by car, keep records locked in the trunk before the start of a trip—don't put them there once at the destination. Where possible, do not leave records unattended, even if they are stored in the trunk. Car trunks are no less accessible to thieves than the front seats.
4. Do not view records in public places where they may be viewed or accessed by unauthorized individuals (e.g., on public transit).
5. Do not leave records open for view in hotel rooms; they should be kept in the hotel safe.
6. Upon returning to the office, immediately replace records containing personal information to their original storage location. Securely destroy any copies that are no longer required.

Guidelines specific to personal information stored on paper-based records when outside the office:

1. Use a sign-out sheet to document who is removing a record, the name of the individual whose personal information is being removed, and the date the record is being removed.
2. If the records are large, consider using a courier to transport it to the destination.
3. Place records in confidential folders, transport them in a secure container, and keep them under control at all times. This includes during meals or breaks.
4. When working from home, keep records locked in a desk drawer or filing cabinet to reduce unauthorized viewing and access by family members or friends.

Guidelines specific to personal information stored on portable electronic devices when outside the office:

1. Protect portable electronic devices containing personal information with a strong password when taken away from the office.
2. Avoid storing personal information on portable electronic devices unless absolutely necessary.
3. To prevent loss or theft, keep portable electronic devices secure at all times, in a locked briefcase, desk drawer, container, or room, and keep them under one person's control at all times. This includes during meals or breaks.
4. When travelling by car, keep all portable electronic devices locked in the trunk before the start of the trip— don't put them there once at the destination. Where possible, do not leave portable electronic devices unattended, even if stored in the trunk.
5. When no longer needed, remove all sensitive personal information from portable electronic devices using a digital wipe utility program. Do not rely on the delete function as the information may still remain on the device.

Guidelines for appropriate use of home computers or portable electronic devices for accessing personal information:

1. Do not use public computers or networks to connect to the office network as these are unsecure devices and locations.
2. Log off from a laptop or home computer and set the automatic log out to occur when not in use.
3. Lock home computers that are used for work-related purposes to a table or other stationary object with a security cable and keep them in a room with restricted access.
4. When accessing electronic records from home, avoid storing any personal information on the hard drive of a home computer. Any personal information that must be stored on hard drives should be encrypted and password protected.
5. Do not share a laptop or home computer that is used for working with sensitive personal information with other individuals, including family members and friends.
6. Ensure that laptops and home computers have, at a minimum, a personal firewall, anti-virus protection, and anti-spyware protection. Ensure that the latest updates and security patches are regularly installed.
7. When conducting business involving personal information over a network, use an encrypted link to the host network, such as a virtual private network (VPN).
8. Ensure that staff do not remove any patient information from the office network without authorization from their supervisor.
9. Watch out for "shoulder-surfing" where unauthorized individuals may casually observe the screen of someone's laptop or desk computer. Consider installing a privacy screen filter to prevent viewing of the screen from an angle.

For additional information, see the BC Information and Privacy Commissioner's release on Physicians and Security of Personal Information, June 2006 at www.oipc.bc.ca.

Managing Contracts and Information Sharing Agreements (ISAs)

This section will:
• Summarize the requirements under PIPA for confidentiality agreements with staff and third parties. • Identify key considerations and elements of contracts with third parties. • Identify key considerations and elements of an information-sharing agreement (ISA).

Service providers, suppliers, partners, employees, and others may be engaged by physicians to assist them in their practices. During their work, these individuals or organizations are likely to be exposed to personal health information in the practice. Therefore, appropriate contractual, confidentiality, or information-sharing agreements (ISAs) are required to ensure that any third parties comply with the practice's expectations and applicable legislation. If they must collect, use, and disclose personal information as part of their contractual obligations, they can only do so with permission. Their responsibilities include using personal information only for the stated purpose, and for no other purpose except as permitted or required by law, and they must notify the practice if any personal information has been lost, stolen, used, or accessed in an unauthorized manner.

Confidentiality Agreements

Under the BC Personal Information Protection Act (PIPA), a physician practice must require internal staff and third parties exposed to personal information to sign a confidentiality agreement. (See the section Ten Steps to Help Physicians Comply with PIPA). These sample confidentiality agreements may be used to support compliance: Confidentiality Agreement for Employees; Confidentiality Agreement for Third Parties; and Confidentiality Agreement for Health Authority Employees working within a Physician Practice.

Guidelines for Contracts

There are a number of considerations for the protection of personal health information when it is exposed to and shared with external service providers (e.g., EMR vendors). Service providers must have permission to collect, use, retain, and disclose personal health information on the practice's behalf. In doing so, the practice is obligated to ensure that personal information continues to be protected.

Before entering into a contract, make sure that:

1. The service providers have effective and comprehensive information privacy practices that they physician office is comfortable with.
2. Contracts include the appropriate privacy protection clauses. These requirements should be monitored and enforced.

When drawing up a contract with a provider, ensure that the following factors are covered:

1. The contract should describe:
    a. All applicable privacy laws and expect the service provider to comply with these as well as their own privacy laws and policies.
    b. All reasonable security measures to protect hardware, software, network, and facilities.
2. The contract should bind service providers to:
    a. Only collect, use, access, and retain the information provided to them as identified in the contract and only allow access to subcontractors that the practice is aware of and has approved.
    b. Allow the practice access to its information when asked for it, and never deny access because of a disputed payment for services.
    c. Report any privacy breach or security incident within an agreed-upon timeframe.
    d. Return or destroy personal information when the contract ends as specified.
3. It is recommended that only service providers who operate their services within Canada be engaged. However, many service providers do operate some or all portions of their services out-of-country for a variety of reasons. Understand where personal information is being stored, who has access, what security provisions are in place, and from what locations personal information may be accessed (e.g., if there is remote access for support). If any aspect of the service provider's operations are to be out-of-country, make sure the contract binds the service provider to BC's privacy requirements as they may not feel compelled to respect privacy laws beyond their own jurisdiction.
4. For specific types of contracts such as for record storage and destruction, see the sections Protecting Personal Information When Leaving a Medical Practice and Secure Destruction of Personal Information.

Guidelines for Information-Sharing Agreements

If personal health information is shared with external organizations or third parties (e.g., external health organizations) on a routine and regular basis, an information-sharing agreement (ISA) must be in place. Clear rules must be established to govern how personal information is exchanged and how to ensure that the least amount of information necessary to achieve a stated purpose is used.

ISAs must also be in place to support new and evolving models for physician practice structures. For example, physicians may organize themselves in different ways when implementing an electronic medical

record (EMR). They may consider creating an EMR for a group practice where it is imperative that there be a clear understanding of who is accountable, who has custody and control, what the rules are for information access and sharing, and security and privacy of personal information.

ISAs usually:

1. Define what personal health information means.
2. Describe the purpose for data sharing.
3. Reference all applicable legislation that provides the legal authority for collection, use, and disclosure of personal information.
4. Establish an understanding of who has custody and control.
5. Identify the type of information that each party will share with each other.
6. Identify the uses for the information and limitations on the uses to the specified purpose.
7. Describe who will have access and under what conditions.
8. Describe how the information will be exchanged.
9. Describe the process for ensuring accuracy.
10. Describe the process for managing privacy breaches, complaints, and incidents.
11. Identify retention periods.
12. Identify secure destruction methods when retention expires.
13. Describe the security safeguards in place to protect information.
14. Describe termination of the agreement procedures.

The Canadian Medical Protective Association (CMPA), in partnership with the Canadian Medical Association, has produced Data Sharing Principles for EMR/EHR Agreements. These principles are intended to provide guidance to physicians in addressing data stewardship and information-sharing issues associated with the variety of contracting scenarios and structures. This document can be found at www.cmpa-acpm.ca/cmpapd04/docs/submissions_papers/com_data_sharing_principles-e.cfm . The College of Physicians and Surgeons of BC has also provided a Data Stewardship Framework that can be found at www.cpsbc.ca .

Responding to a Privacy Breach—Key Steps for Physicians

This section will:
• Explain what constitutes a privacy breach. • Identify whistle-blower protections in the regulations. • Identify the four steps that physicians in private practice need to take following a suspected or confirmed breach. • Explain the role of the Information and Privacy Commissioner for BC in regards to breaches.

A privacy breach occurs when there is unauthorized access to, collection, use, disclosure, retention, or destruction of personal health information. The following are some common examples of privacy breaches:

- Personal information is stolen or misplaced.
- A paper chart is lost or stolen.
- A letter is inadvertently mailed to an incorrect address or faxed to the wrong person.
- An electronic portable device (e.g., laptop, handheld electronic device, USB storage device) is lost or stolen where appropriate security controls such as passwords or encryption have not been implemented.
- Inappropriate access to personal information is stored in an electronic system.
- Personal information is not disposed of appropriately.
- A person who legitimately accesses records gains unintended access to information that he or she is not authorized to see.

Suspected or real privacy breaches can come to a practice's attention through a complaint by a patient or member of the public, through the Office of the Information and Privacy Commissioner for BC (OIPC) as a result of a formal complaint, or through compliance monitoring mechanisms such as audit trails in electronic systems alerting to unusual access.

Anyone who reports a privacy breach is protected under whistle-blower protection embedded in privacy legislation. This protects an individual from being dismissed, suspended, demoted, disciplined, harassed, or otherwise disadvantaged for having reported the breach.

Once a breach is reported, it must be responded to immediately. There are four key steps in responding:[3]

Step 1: Contain the breach

1. Contact the designated Privacy Officer.
2. Notify law enforcement if the breach involves theft or criminal activity.
3. Immediately contain the breach, which could involve suspending a user account to an electronic system, shutting down the system that was breached, and/or retrieving the documents.

Step 2: Evaluate the risks associated with the breach

Within two days of discovering a breach, to determine what further steps are necessary, consider the following factors:

1. What kinds of personal information are involved?
2. What format was the information in (paper, electronic) and how was it protected (encrypted, anonymized, password protected)?
3. Was it lost or stolen or mistakenly disclosed?
4. Can the personal information be misused?
5. What is the cause of the breach?
6. Is it an isolated event or is there a risk of ongoing or further exposure?
7. Who and how many individuals are affected by the breach?
8. Is there a relationship between the unauthorized recipients and the data subject? A close relationship between the victim and the recipient could increase the likelihood of harm.
9. Is there risk to public health and/or safety as a result of the breach?
10. Has the information been recovered?

A Privacy Breach Checklist is available from the Office of the Information and Privacy Commissioner for BC (OIPC) to support a response to a privacy breach (go to www.oipc.bc.ca).

Step 3: Implement notification procedures

Contact the OIPC prior to establishing any next steps for breaches that appear to be media-sensitive and/or carry risks of identity theft. The following factors are relevant in deciding whether to report a breach to the OIPC:

1. The sensitivity of the personal information.
2. Whether the disclosed information could be used to commit identity theft.
3. Whether there is a reasonable chance of harm from the disclosure including non-pecuniary losses.

[3] Key Steps in Responding to Breaches, Office of the Information and Privacy Commissioner for BC, June 2008, www.oipc.bc.ca

4. The number of people affected by the breach.
5. Whether the information was fully recovered without further disclosure.

Individuals affected by a privacy breach should be notified to avoid or mitigate harm to them. The decision to notify is determined by responding to the questions in Step 2. This step, if appropriate, should take place within one week of discovering the breach. A standard Breach Notification Assessment Tool[4] is also available to assist in determining if notification is necessary.

Who should be notified:

1. Individuals (whether patients or staff) whose personal information is involved in the breach.
2. Other organizations that are or may be affected by the breach.

Other groups may also require notice based on legal, professional, or contractual obligations. In the case of self-governing professions, contact the regulatory body as it may receive calls from the public concerning the breach. It may also be prudent to notify the College of Physicians and Surgeons of BC.

What to include in the notification:

1. A description of what occurred.
2. The elements of personal information involved.
3. The steps taken to mitigate the harm.
4. Advice to affected individuals on what they can do to further protect themselves and mitigate the risk of harm.
5. A statement of their right to complain to the College of Physicians and Surgeons of BC or the Office of the Information and Privacy Commissioner for BC (OIPC) .

Step 4: Prevent future privacy breaches

Once immediate steps are taken to mitigate the risks, the practice, including the staff, should take time to investigate the cause of the breach. Long-term safeguards should be developed to prevent further breaches. Privacy and security policies may need to be updated and staff should be refreshed on their privacy obligations through training and education. **This process should take place within two months of the breach.**

[4] Breach Notification Assessment Tool. Office of the Information and Privacy Commissioner for BC and Information and Privacy Commissioner of Ontario, December 2006, www.oipb.c.ca or www.ipc.on.ca

Responding to Patient Requests to Access Personal Information

This section will:
• Explain patients' rights about accessing their personal information held in a physician's office. • Identify the parameters that apply to how a physician responds to such a request, including timelines, exceptions, and applicable fees.

Under the BC Personal Information Protection Act (PIPA), patients (or the patient's legally authorized representative) are entitled to access their personal information in the control of a physician's office, to ensure its accuracy and completeness, to understand how their information has been used, and to identify the names and the organizations to which their personal information was disclosed.

A patient must make a request for access to personal information in writing, and the physician's office must respond within 30 working days of receiving a request. (See the Patient Request Form for Access to Personal Information.) The response may be a copy of the information or, in the case where copies cannot be made, arrangements must be made for the patient to review the original records.

A physician office may charge a reasonable fee for such access. Where a fee is charged, a written estimate must be provided to the patient, which may request that a deposit for all or part of the fee be paid before the service is provided.

There are some exceptions in which personal information may not or must not be released to a patient. For example, personal information that is protected by client-solicitor privilege or that would reveal confidential business proprietary information is not required to be disclosed. Further, information must not be disclosed in certain situations where doing so may result in harm to a patient or someone else, or if the personal information is about someone else. If access is refused, the appointed Privacy Officer or delegate must explain to the patient the reasons why.

The designated Privacy Officer must educate staff on the appropriately response to such requests. A patient may request a review of a response that he or she is not satisfied with **within 30 working days**, by going back to the physician's office. If the complaint cannot be resolved, the patient may ask the College of Physicians and Surgeons to resolve the matter. A patient may also escalate the complaint to the Office of the Information and Privacy Commissioner for BC (OIPC) at www.oipc.bc.ca.

Ensuring Accuracy of Patient Records

This section will:
• Identify the requirements on keeping paper and electronic records accurate. • Explain patients' rights to verify accuracy of their records and ask for corrections.

Regardless of the method used to record patient health information, physicians must ensure that the information is up-to-date and accurate. Patient information must be documented in the record as soon as possible after an event has occurred, providing current information on the care and condition of the patient. The clinical consequences of inaccurate personal health information range from personal embarrassment to physical harm or even death.

Under the Personal Information Protection Act (PIPA), patients have the right to request their personal health information be corrected if they believe it is not accurate or complete. Of course, professional or expert opinions cannot be corrected or changed.

The practice's privacy policy must be openly available, must describe how patient information is kept accurate, and must describe how patients may request correction to their information. Patients (or their legally authorized representative) may make a request for correction in writing (see the Patient Request Form for Correction of Personal Information) and physicians' offices must respond **within 30 working days** of receiving a request. If appropriate, an amendment is made and a copy of the amendment is sent to each organization to which the inaccurate or incomplete information was disclosed within the past year. If no correction is necessary, the designated Privacy Officer or delegate must explain the reasons to the patient.

The designated Privacy Officer must educate staff on how to appropriately respond to such requests. If a patient is not satisfied with the outcome, he or she may request a review by the College of Physicians and Surgeons of BC or take the matter to the Office of the Information and Privacy Commissioner for BC (OIPC) .

Patient information in physician records should:

1. Be written clearly, legibly, and in such a manner that it cannot be erased.
2. Have any alterations or additions dated, timed, and signed in such a way that the original entry can still be read clearly.
3. Be accurately dated, timed, and signed, with the name of the author printed alongside the first entry.

4. Be readable on any photocopies or faxes.
5. Be written, wherever possible and appropriate, with the involvement of the patient.
6. Be clear, unambiguous, and written in terms that the patient can understand. Abbreviations, if used, should follow common conventions.
7. Note clearly, if applicable, reasons for not making a correction indicating a correction was requested but not made.
8. Be consecutive.

Other medical observations must also be included, such as examinations, tests, diagnoses, prognoses, prescriptions, and other treatments.

In addition to the above requirements, Electronic Medical Records (EMRs) should:

1. Have the ability to correct information through an amendment. The original data must not be modified or deleted; it should be maintained as history.
2. Accurately date and time-stamp a correction, recording who made the amendment.
3. Allow for notation, if applicable, that a correction was requested but not made.
4. Be able to generate a copy of a patient record with the amended data and correction history.

Managing Patient Complaints

This section will:
• Explain patients' rights regarding complaints related to their privacy. • Identify the requirements of an effective complaint management process. • Describe the 10 steps of managing a complaint.

Under the BC Personal Information Protection Act (PIPA), physicians' offices must have a complaint management process for individuals who have concerns about the office's privacy practices. Having an accessible and effective complaint management process is an important aspect of managing privacy risks and helps to promote accountability, openness, and trust. It also allows an office to address complaints in a timely manner,[5] identify systemic or ongoing compliance issues, and demonstrate commitment to privacy.

When setting up a complaint management process, consider the following:

1. Decide who in the office will be responsible for receiving and managing complaints about the office's compliance with PIPA. This could be the appointed Privacy Officer, or it could be delegated to another individual.
2. Develop and document a complaint procedure that is accessible, simple, and easy to use.
3. Consider developing a complaint form to assist in recording the complaint and to collect the necessary information required to investigate and respond.
4. Ensure that all staff are aware of the complaint management process so that they can direct the complainant to the appropriate person for follow-up, or in the absence of this individual, provide information to the complainant on how they may proceed with a complaint.
5. Remember that addressing a complaint quickly allows to maintain or even increase the patient's trust in the practice.

Ten steps for managing a complaint:

1. When the complaint is received in writing, record the date of the complaint and acknowledge its receipt.
2. If the complaint is received verbally, record the nature of the complaint and the details.
3. If necessary, contact the individual to clarify the complaint.
4. Ensure that the complaint process is fair, impartial, and confidential.

[5] See recommended timeframes for managing privacy breaches in the Privacy Breach Management Policy Template, Office of the Information and Privacy Commissioner of BC, June 2008, available at www.oipc.bc.ca.

5. Investigate the complaint by gathering information and fully understanding the circumstances. Clarify specifics of the complaint by asking questions such as:
    a. What do you believe occurred?
    b. What personal information is involved and what happened to it?
    c. When and where did the event(s) occur?
    d. Who was involved (e.g., staff, locum physicians, visiting specialists, physicians-in-training, third party contractual staff)?
6. Where a complaint is justified, determine the specific cause and take measures to remediate the situation. Communicate this to relevant staff involved. Record all decisions and actions taken to prevent recurrence.
7. If a complaint cannot be substantiated, document the investigation so it can be explained to the complainant.
8. Notify the complainant of the outcome regardless of whether the complaint can be substantiated or not. Where applicable, inform him or her of the steps taken to rectify the concerns.
9. Inform the complainant of the right to appeal to the Information and Privacy Commissioner for BC if he or she is not satisfied with the office's response to the complaint.
10. If applicable, prevent recurrence through techniques such as modifying or updating policies and procedures, providing staff training, and implementing improved privacy and security safeguards.

Secure Destruction of Personal Information

This section will:
• Describe best practices for the secure destruction of personal information. • Identify key considerations and elements of contracts with a service provider to support the destruction of records.

Under the BC Personal Information Protection Act (PIPA) a physician's office is expected to securely dispose of personal information that is no longer required to prevent unauthorized access, inappropriate use, or identity theft. The goal is to permanently destroy personal information or irreversibly erase it so that the information cannot be reconstructed, whether in paper or electronic format. This includes the original records and any duplicate copies of records that may have been created for in-office use. A service provider may be contracted to provide the record destruction services.

Best Practices

Best practices for the secure destruction of personal information include the following:

1. Dispose of paper records securely by cross-cut shredding. Don not use single-strip, continuous shredding because it is possible to reconstruct the strips. If practical, consider incinerating paper records.
2. Dispose of personal information stored on electronic devices (such as disks, CDs, DVDs, USB storage devices, and hard drives) securely by physically damaging the item and discarding it, or by using a wipe utility to remove the original information. Note that a wipe utility may not completely erase the information.
3. If office machines such as photocopiers, fax machines, scanners, or printers contain storage devices, ensure that they are overwritten, erased, removed, or destroyed when the machines are replaced.

Using a Service Provider to Destroy Records

When contracting a service provider to support the destruction of records, look for one that is accredited by an industrial trade association such as the National Association for Information Destruction (www.naidonline.org). Check the references of any service provider and insist on a signed contract. The contract should cover these key points:

1. Clearly describe the responsibilities of the service provider for the secure destruction of the records involved.
2. Describe how the service provider will collect the records from the physician's office.

3. Describe how the destruction will be accomplished for the records involved.
4. Upon request, provide a certificate of destruction documenting date, time, location, operator, and destruction method used.
5. Allow an authorized person from the physician's office to visit the facility and/or witness the destruction upon request.
6. Require—or request proof of—employees receiving training on the importance of secure destruction of confidential personal information.
7. Require that if the provider is subcontracting the destruction to a third party, that notice be provided ahead of time with a contract in place with the third party consistent with the service providers' obligations to the physician's office. The service provider must remain liable for all services performed.
8. Describe the secure storage of records pending destruction.
9. Specify the limited timeframe upon which records will be destroyed.

(For more information, see the section Guidelines for Managing Contracts and Information-Sharing Agreements. Also check the BC E-waste: End-of-Life Electronic Equipment Recycling Program at www.rcbc.bc.ca/education/hot-topics/e-waste.)

Finally, while PIPA does not include the FIPPA provisions regarding prohibition of storage and access to personal information from outside Canada, it is recommended that service providers operating within Canada be engaged. However, many service providers do operate some or all portions of their services outside the country, for a variety of reasons. Be sure to understand where personal information is being stored, who has access to it, what security provisions are in place, and from what locations personal information may be accessed (e.g., if there is remote access for support). If any aspect of their operations are to be out-of-country, make sure the contract binds the service provider to BC's privacy requirements as they may not feel compelled to respect privacy laws beyond their own jurisdiction.

Protecting Personal Information When Leaving a Medical Practice

This section will:
• Describe best practices regarding privacy when leaving a medical practice. • Identify key considerations and elements of contracts with a service provider to provide storage, retrieval, or destruction of records.

When a medical practice is closed, replaced, or relocated, physicians have a professional and legal duty to use reasonable efforts to arrange secure transfer of patient records to another provider that agrees to accept the responsibility, to arrange secure storage and retrieval of patient records for the remaining retention periods, or to securely dispose of records where the retention period no longer applies. Physicians must also ensure continuity of care for those patients who require it.

There are guidelines specific to leaving a medical practice available on the College of Physicians and Surgeons of BC website, in the Resource Manual: www.cpsbc.ca/files/u6/Leaving-Practice.pdf.

Specific considerations for protecting personal information when leaving a medical practice include the following:

1. Ensure that the patient notification includes information on the departure date, the process for how patients can obtain a copy of their records or request transfer of a copy of their records to a new physician, and how they may access any records stored by a service provider. A reasonable fee may be charged for providing this service and this charge should be communicated to the patient.
2. With patient authorization, only transfer a copy of the patient record to the new physician.
3. Ensure that the original record is retained under College retention guidelines for the purposes of future complaints or legal action. It is suggested that patient records be retained for at least seven years from the date of last entry or, in the case of minors, seven years from the time they would have reached the age of majority. In a group practice, it is possible the group will undertake custody of the records, especially if patients continue to attend the practice.
4. For accuracy and completeness, make sure that all patient record documentation is completed before records are archived.
5. Ensure there is a process in place to support any outstanding patient work that may be in progress (e.g., pending tests that may require follow-up).
6. If the records are no longer required, follow secure records disposition procedures. (See the section Secure Destruction of Personal Information.)

If a service provider is engaged to provide storage and retrieval services for patient records for the remaining retention period, ensure that this is done under a legal agreement with the following provisions:

1. Maintain the confidentiality of all patient information stored, providing access to information only to authorized representatives of the physician or with written authorization from a patient or legal representative.
2. Upon request of the physician, promptly return all confidential patient information without retaining copies.
3. Prohibit the use of patient information for any purpose other than what was mutually agreed upon. This includes selling, sharing, discussing, or transferring any patient information to unauthorized business entities, organizations, or individuals.
4. Provide a secure storage facility that protects against theft, loss, damage, and unauthorized access.
5. As specified by the physician, securely destroy patient information at the end of the retention period.

While PIPA does not include the FIPPA provisions regarding prohibition of storage and access to personal information from outside Canada, it is recommended that physicians avoid disclosing personal identifiable information outside of Canada and prohibit access to such records from outside Canada without expressed patient consent. Such a clause can be added to the contract with a service provider.

Use of Fax by Physicians

This section will:
• Summarize the benefits and risks associated with using a fax in the clinical context. • Identify key considerations when using faxes to transmit personal information.

In today's clinical setting, faxes are commonly used to transmit health information. For example, a laboratory may fax a patient's medical test result to a physician, or a physician may fax a copy of the patient's medical record to a specialist who intends to treat the patient.

Under the BC Personal Information Protection Act (PIPA) steps must be taken to reduce the risks associated with faxing personal information and reasonable safeguards must be in place to protect personal information from unauthorized collection, use, and disclosure.

What Are the Risks?

Faxing increases the risk that sensitive personal information could be read by individuals other than those for whom they were intended. This might occur when, for example, personal health information such as a medical diagnosis, is sent to an incorrect fax number (caused by misdialing or by pressing the wrong speed-dial key), or when information is exposed to unauthorized individuals simply because the fax machine is located in an open, unsecured location. Fax transmissions can also be tapped into and monitored similar to a telephone call.

How to Reduce the Risks

A fax sent to another physician or hospital about urgent or significant patient issues should not be considered a substitute for effective and efficient communication. Faxes can be missed, may not reach their designation, or may remain in receiving trays if the recipient is unavailable. Here are some steps to reduce the risks:

1. Establish an office policy on faxing and ensure that staff are trained on the appropriate use of the fax machine and faxed documents.
2. Fax personal health information only when it is absolutely necessary and when the information must be transmitted immediately, and only if the information is something that could be comfortably discussed over the telephone with a patient.

3. Ensure that any fax machine used to send or receive personal information is "dedicated" and located in a secure area to prevent unauthorized persons from viewing or receiving the documents. Sharing fax machines, particularly where personal information is frequently sent and received, is discouraged.
4. If sending personal information by fax modem (a fax device contained in a computer), confirm that the other users of the computer cannot access the fax program without a password. Consider using encryption.
5. Always use a fax cover sheet that identifies both the sender and recipient with contact information and states the total number of pages being sent.
6. Include a disclaimer stating that the faxed material is confidential and only intended for the stated recipient. This disclaimer should also state that anyone receiving the fax in error must immediately notify the sender and return or destroy the fax, as per the request of the sender.
7. Before faxing the information, confirm the recipient's fax number and ensure that the recipient has taken appropriate precautions to protect the personal information upon receiving it.
8. If using pre-programmed fax numbers, regularly verify these numbers to ensure they are accurate and up-to-date.
9. After dialling a fax number, including a pre-programmed number, confirm the number before sending the fax.
10. Remove documents sent by fax as soon as they have been processed. Do not leave the material sitting on or near the fax machine.
11. Check the fax confirmation report as soon as the fax has been sent to confirm that the fax went to the correct place and that all pages were transmitted and received.
12. If a fax is received in error, promptly notify the sender and return or destroy the information as requested by the sender.

If a fax containing personal information is sent to the wrong number or person, follow these steps:

1. If the information cannot be retrieved or destroyed, notify the person responsible for privacy compliance in the office.
2. Follow procedures for managing privacy breaches. (See the section Responding to a Privacy Breach—Key Steps for Physicians).

If someone asks the physician's office to fax his or her personal information, be sure to follow these steps:

1. Identify the person making the request with certainty and advise him or her of the preference to provide the data in a more secure fashion (e.g., photocopies sent by mail or courier).
2. Explain how faxing personal information can result in accidental disclosure or interception by other people not intended to receive it.

3. Explain the precautions that have been taken to reduce the risks and ensure the person consents before the personal information is faxed.

Maintenance of Faxed Documents

When planning a document maintenance policy, consider the following:

1. Do not make or keep more copies of faxed material than needed.
2. Securely destroy extra copies that are no longer needed.
3. Ensure that personal health information that has been faxed becomes part of the patient's medical record and follow appropriate retention guidelines.

As well, consider these additional factors:

1. Where possible, use alternative and secure methods of delivering personal information, particularly if it is sensitive.
2. If faxing sensitive personal information on a frequent basis, use a secure fax machine that has encryption and other security measures.
3. Use the feature that requires the receiver to enter a password before the machine will print the fax to ensure that only the intended receiver can retrieve the document.
4. Appoint one individual in the office to be responsible for sending and receiving faxes. This individual can check each day's fax history report for errors or unauthorized faxing.
5. Arrange a time to receive faxes so that someone can be at the fax machine when they arrive.
6. Phone the recipient to confirm that he or she is the right person to receive the fax, that he or she will be there to receive the fax, and to confirm the fax number. Have the recipient call back to confirm receipt.
7. Use unique identifiers or codes to protect the identity of the individual whose personal information is being sent by fax.

Use of Email by Physicians

This section will:
• Summarize the benefits and risks associated with the use of email in the clinical context. • Identify key considerations required when using email for transmitting personal information. • Identify key considerations required if planning to use email communication with patients.

The use of email for communication in medical offices has in some cases become as common as fax. Email is a quick and efficient method for sharing information between providers and between providers and patients. When used in addition to face-to-face communication, email can enhance the patient-provider relationship. It can reduce non-essential office visits and save time otherwise spent communicating by phone. Email permits both parties to read and respond when it's convenient, and it also allows supporting documents to be attached, if necessary.

Steps must be taken to reduce the risks associated with email communication and ensure that reasonable safeguards are in place to protect personal information exchanged via email.

What are the risks?

In general, any type of email communication has some embedded risks:

1. An email message, because it is usually not encrypted, can be intercepted. It can also be altered and forwarded to unintended recipients or delivered to the wrong address.
2. Email messages containing personal information can be sent or received from unsecure locations such as a publicly accessible computer or a home computer. These messages could be retained on the home computer or in files maintained by Internet service providers. People other than the intended recipient may have access to the email account.
3. Attachments associated with an email may contain viruses that could cause serious damage to computer systems.
4. Email backup services and organizational retention rules may expose the information beyond what was intended.
5. The information being emailed may leave Canada during the email transition and become subject to other legislation or be affected the absence of legislation.

There are several additional risks to patient-provider email communication:

1. It can be difficult to confirm the identity of the patient in an email request. A patient's name without additional identifiers may be insufficient as patients may have similar names and email addresses.
2. If a patient does not receive a response in a timely manner, there may be adverse health consequences such as not getting the medical help needed on time.
3. A certain level of patient literacy is required for the email exchange to be beneficial and efficient.
4. The content of an email can be misinterpreted, which could lead to adverse health consequences or even a complaint or legal action if the patient's perception is one of inadequate or ineffective communication.

How to Reduce the Risks

Email sent to another physician or hospital about urgent or significant patient issues should not be considered a substitute for effective and efficient communication as there is no assurance the recipient will access the account regularly.

Before emailing personal information, take the following precautionary steps:

1. Confirm that you have the correct email address for the intended recipient. Verify email addresses regularly as they are not always intuitive, can be duplicated, and frequently change.
2. Where feasible, the recipient of the email should be contacted and informed that confidential information is being sent. Have the recipient call back to confirm receipt.
3. When emailing sensitive personal information consider using unique identifiers or codes to protect the identity of the individuals involved. Unsecured email messages can be read during transmission.
4. Ensure that confidential and sensitive personal information sent by email is encrypted with access provided only to authorized individuals who have the access code.
5. Add a confidentiality disclaimer to email messages that states that the content is confidential and only intended for the stated recipient. It should also state that anyone receiving the email in error must notify the sender, and return or destroy the email as per the request of the sender.
6. Protect any attached documents with a strong password and notify the recipient by phone of the password.
7. As sender, be aware of the security of the receiving email account and who has access to it.
8. Ensure that each email inbox used to send or receive messages has a secure password known only by the individual authorized to access that inbox.
9. Never use email distribution lists to send personal information.

Finally, While PIPA does not include the FIPPA provisions regarding prohibition of storage and access to personal information from outside Canada, it is recommended that physicians avoid the disclosure of personal identifiable information outside of Canada and prohibit access to such records from outside Canada without expressed patient consent.

Before agreeing to implement patient-physician email communication, take the following steps:

1. Thoroughly consider the advantages and disadvantages of email communication with patients before offering this service.
2. Where possible, use alternative and secure methods of delivering personal information, particularly sensitive information. Do not email sensitive information such as personal health information unless absolutely and immediately necessary.
3. Establish an office policy on email and ensure that:
    a. It includes criteria for the patient-provider communication, acceptable use, email etiquette, and management of email documentation as part of the patient's medical record.
    b. Staff are trained on the appropriate use of email and maintenance of emailed documents.
4. Develop policies and procedures:
    a. To inquire about the patient's literacy and ability to use email effectively.
    b. To obtain the patient's consent to the use of email as a method of communication.
    c. To educate patients about the appropriate use of email for this purpose.
    d. On termination of a patient from email communication.
5. Address security risks by implementing encryption technologies, email access codes, and other measures to protect against unauthorized access.

If an email containing personal information is sent to the wrong address or recipient, follow these steps:

1. Contact the person responsible for privacy compliance in the office.
2. Follow procedures for managing privacy breaches. (See the section Responding to a Privacy Breach—Key Steps for Physicians.)

If someone asks the physician office to email his or her personal information, be sure to follow these steps:

1. Identify the person making the request with certainty and advise him or her of your preference to provide the data in a more secure fashion (e.g., photocopies sent by mail or courier).
2. Explain how emailing personal information can result in accidental disclosure or interception by other people not intended to receive the information.
3. Explain the precautions that have been taken to reduce the risks and ensure the person consents before emailing the personal information.

Maintenance of Email Documents

When planning an email maintenance policy, consider the following:

1. Do not make or retain more copies of email communications than needed.

2. Securely destroy extra copies that are no longer needed.
3. Ensure that personal health information emailed becomes part of the patient's medical record and follow appropriate retention guidelines.

Photography, Videotaping, and Other Imaging

This section will:
• Describe reasonable practices for protecting personal information privacy when using photography, videotape, digital imaging, or other visual recordings. • Identify what needs to be done before, during, and after the photography or recording session.

The following guidelines should be followed when using photography, videotape, digital imaging, or other visual recordings during consultations between physicians and patients, for the purposes of care of that patient, for education, or for research.

Medical, surgical, or any other procedures involving patients who may be identified may be photographed or recorded on videotape or on film for the purposes of care **only** when the patient has given explicit written consent. This consent does not authorize the use of the images for any other purposes such as education including through scientific publication or research; separate consent is required for each such purpose.

Before the photography or recording session, physicians are responsible for ensuring the following:

1. That the patient is given time to consider a consent form and explanatory material that provides relevant information in a way that the patient can understand (translations should be provided where necessary prior to signing the form).
2. That the patient understand the purpose for which the photograph or recording will be used, who will be allowed to see it, whether copies will be made, and how long the photograph or recording will be kept.
3. That the patient understands that refusal to consent will not affect the quality of care being offered and that his or her consent can be withdrawn at any time (i.e., it is revocable without consequence).
4. Where patients are deemed incapable or incompetent, that consent be sought from a close relative or personal representative. In the case of children, the consent of a parent or guardian must be obtained.

During the photography or recording session, physicians are responsible for the following:

1. Ensuring that the photography or recording be stopped immediately if the patient requests or if, in the physician's opinion, the session is reducing the benefit which the patient might derive from the consultation.

After the photography or recording session physicians are responsible for ensuring the following:

1. That the patient is invited to consider whether he or she wishes to withdraw consent to the use of the photograph or recording. If the patient does withdraw consent, the physician should ensure that the photograph or recording is securely destroyed or erased as soon as possible.
2. That the photograph or recording is used only for the purpose for which the patient's consent has been given.
3. That photographs be filed with the patient's record. Videotapes or recordings, because of their size, may need to be stored separately in a secure area. If not stored with the patient's record, a note should be made on the patient's chart indicating the location of the photos, recordings, or images. All photographs, videotapes, recordings, or images must be identified with the patient's name, identification number, and date.
4. That photographs, videotapes, recordings, or images are stored with the same level of security required for all confidential medical records.
5. Where photographs, videotapes, recordings, or images may be shown to people other than the immediate health care team responsible for the care of the patient, that the following additional safeguards are applied:
    a. The patient must be made aware of and understand that the photographs or recordings may be shown to people with no responsibility for his or her health care.
    b. The patient must be offered the opportunity to view the photographs or recordings in the form in which they are intended to be shown, and have the right to withdraw consent.

Where it is proposed that a photograph or recording be used in which the patient cannot be identified, it is sufficient for the physician to provide the patient with an oral explanation of the purpose of the proposed recording and recording the patient's chart. No photograph or recording should be made contrary to the patient's wishes.

In exceptional circumstances, where no photography or recording of a procedure has been planned but an unexpected development during the procedure makes photography or recording highly desirable for educational purposes, photography or recording may be made without consent if the patient's consent cannot be obtained (e.g., due to the patient being under anaesthesia). The patient's consent must subsequently be obtained before use is made of the recording.

Secondary Use of Personal Information for Research

This section will:
• Summarize the requirements under PIPA regarding consent for research and the exceptions where consent is not required. • Identify key considerations for physicians who have patients participating in research projects.

Maintaining patient confidentiality is a fundamental responsibility of any physician practice and is at the core of the patient-physician relationship. Although the patient owns his or her personal health information, physicians act as custodians accountable for medical information they collect and retain, and must protect its disclosure through obtaining appropriate consent.

While the BC Personal Information Protection Act (PIPA) does not require expressed consent for direct patient care (it is implicit), physicians must obtain patient consent for the collection, use, or disclosure of personal information for other use such as research. This does not include contact information or work product information; personal information is information about an identifiable individual and includes personal health information.

If a practice collects, uses, or discloses identifiable patient information internally for research purposes, it must obtain the written consent of the patient subject to certain exemptions. If a practice discloses identifiable personal information to a third party for research purposes, it must usually obtain written consent of the patient. In rare cases, it is possible to proceed without the consent of an individual, subject to specific exemptions under PIPA that permit the collection, use, and disclosure of personal information when the following conditions are present:

1. The research purpose cannot be accomplished unless the personal information is provided in an individually identifiable form.
2. The disclosure is on condition that it will not be used to contact persons to ask them to participate in the research.
3. Linkage of the personal information to other information is not harmful to the individuals identified by the personal information and the benefits to be derived from the linkage are clearly in the public interest.
4. The organization to which the personal information is to be disclosed has signed an agreement to comply with the following:
    a. The Personal Information Protection Act (PIPA).

b. The policies and procedures relating to the confidentiality of personal information of the organization that collected the personal information.
c. Security and confidentiality conditions.
d. A requirement to remove or destroy individual identifiers at the earliest reasonable opportunity.
e. Prohibition of any subsequent use or disclosure of that personal information in individually identifiable form without the expressed authorization of the organization that disclosed the personal information.

5. It is impracticable for the organization to seek the consent of the individual for the disclosure.

The disclosure of identifiable patient information for research, where the research could not reasonably be accomplished without identifiable data, requires the approval and review of an approved research ethics board. Without such a review, the practice must refrain from disclosing identifiable patient data.

Key Considerations

The following are key considerations of the secondary use of personal information for research:

1. In all but the exceptional circumstances outlined above, patients must be provided with information related to the research opportunity and be asked for written consent.
2. Personal information approved for research purposes should, even with explicit consent in hand, be de-identified to whatever extent is feasible and practical.
3. Records must be returned or securely destroyed when the research is complete.
4. If a patient withdraws his or her consent to the collection, use, or disclosure of personal information for research purposes, the practice must stop collecting, using, or disclosing the information unless permitted under PIPA. If a patient decides to withdraw his or her prior consent for research purposes, the patient must contact the practice's Privacy Officer.
5. If a patient believes his or her personal information has been inappropriately collected, used, or disclosed for research purposes without his or her consent, he or she may bring the matter to the practice's Privacy Officer for review and investigation. If the patient believes the matter has still not been resolved, he or she may bring the concern to the College or to the Office of the Information and Privacy Commissioner for BC (OIPC).

Privacy and Security Considerations for EMR Implementation

This section will:
• Summarize privacy and security considerations during the transition from paper to EMRs. • Identify key privacy and security best practice features of an EMR.

The transition from a traditional paper-based patient record to an Electronic Medical Record (EMR) is a significant undertaking, requiring changes to a practice from many perspectives—clinically, administratively, and organizationally. Physicians must be prepared to maintain the protection of personal health information during the transition period where both paper and electronic versions exist in parallel.

Making the Transition

During the transition to an EMR, consider the following:

1. Understand existing paper-based workflow processes including data flow, and modify practices as necessary to integrate the use of an EMR and achieve the greatest benefits.
2. Assess existing privacy and security policies and practices and revise them to reflect the use of an EMR and personal information in electronic format.
3. Update staff privacy training to incorporate an understanding of the changes associated with an EMR.
4. To begin the transition to an EMR, either scan paper records into electronic format, or start entering data into the EMR beginning on day one. Either way, the College recommends that paper records be kept in close proximity for at least six months. Unless they are completely scanned into the EMR, paper records must be kept as per College retention guidelines.
5. Ensure that patients still have access to their complete information upon request, even if the information now exists in a combination of formats (paper, electronic, digital).

Privacy and Security Considerations

EMR software should have the following features which have become industry standards and should be implemented to support the protection of patient health information:

1. Roles-based access control (see the section Electronic Medical Records and Roles-Based Access),
2. Audit trails to record user access.
3. Allowance for correction/amendment of information.
4. Ability to mask/unmask sensitive data (see the section Consent and Disclosure Directives in BC).

5. User account management including unique user IDs and passwords.
6. Automatic log off feature.
7. Confidentiality disclaimers on printed reports.
8. Robust backup and recovery procedures.

Privacy and Security of Wireless Technology

This section will:
• Define wireless technology and its risks and benefits. • Identify key considerations regarding the use of wireless technology in the context of a physician office.

Wireless technologies are increasing in popularity and there are a growing number of applications available that are related to health care. These technologies allow physicians to monitor and provide care to their patients remotely. For example, physicians could, through wireless technology, remotely monitor a patient's chronic condition by detecting and responding to problems as they occur. The technology also increases efficiencies by allowing physicians remote access to Electronic Medical Record (EMR) systems from any location.

While there are benefits to using wireless technology, there are also questions about the risks to privacy and security of personal information. For example, how can patients and providers be sure that only authorized individuals have access to information? How can sensitive personal information be accurately and securely transmitted? What happens if a wireless device is lost or stolen?

Under the BC Personal Information Protection Act (PIPA), physicians must implement reasonable and appropriate safeguards to protect the privacy and confidentiality of personal information, particularly personal health information, regardless of format.

Key Considerations

The following are key considerations of using wireless technology:

1. Wireless fidelity (Wi-Fi) refers to a range of technologies for wireless data networking. Wireless data networking links computers without wires. For example, wireless routers are commonly used in home or small office computer networks. Personal information transmitted over these wireless networks can be intercepted. Up-to-date encryption is recommended for transmitting personal information to minimize the risk of unauthorized interception.
2. Wireless technology can be embedded in or attached to a chip such as a radio frequency identification (RFID) chip. Where a RFID chip collects or uses personal information, it is important to ensure that strong encryption is in place and that the systems to which the device is connected provides adequate end-to-end security.

3. If personal health information is stored on a wireless device such as a laptop computer, the information should be encrypted and access protected with a user ID and password.
4. Cell phones and Blackberry devices are also categorized as wireless technologies as they can be used to send or store emails or instant text messages. These devices must be set up to operate securely, including encryption of data transmissions and password protection.
5. Any wireless device connected to a network can serve as an illicit entry point for the entire network if it is not properly set up with the appropriate security controls.

Electronic Medical Records and Roles-Based Access

This section will:
• Define roles-based access and identify key considerations related to its implementation. • Identify best practice additional privacy and security controls that support implementation of the roles-based access to the EMR.

Roles-based access control is a highly recommended functionality and is available in most Electronic Medical Record (EMR) systems used today. Roles-based access controls use technology to strengthen the relationship of trust between the physician and patient by ensuring that access to the patient record is based on the "need to know" principle.

The objective of a roles-based access model is to identify all possible roles that require access to patient health information, to which a standard set of functional patient information areas (e.g., lab results, medication information, registration information) and permissions (e.g., reading, writing, printing) can be assigned. Having this model defined also allows for ease of account management when setting up new users and modifying accounts. Roles-based access models must be designed to support both business and clinical workflow, and as such the EMR software must have flexibility to support the unique needs of each physician's office. It must also allow for exceptions to the standard roles and permissions as long as it is authorized and necessary for the performance of job duties.

Roles can be defined for all of the various individuals, whether employees or not, who access the EMR. These include clerical staff, billing services, office nurses, students, residents, physicians-in-training, locum physicians, on-call group, visiting specialists, and other physicians within the practice.

An additional important concept is that a role alone does not entitle an individual to access a given record; there needs to be a need to know based on a legitimate relationship with the patient. "Need to know" frequently becomes "want to know," however, so when assigning roles a prudent physician will always assess the degree to which access to the personal information is truly necessary to perform one's duties.

The following factors should be considered when defining roles, functional area of information access, and permissions associated with roles:

1. What are all the possible roles that would require access to patient information in the office?
2. What are the possible functional areas of information that may need to be accessed (e.g., clerical, clinical, financial/billing)?
3. What are all the possible permissions that could be assigned to each role (e.g., create, read only, update, delete)?
4. Are there additional permissions that a user in a role could be assigned (e.g., mask/unmask information, print, email)?

The following questions should be considered when determining what functional areas and permissions should be assigned to each role, and thereby assigned to a user:

1. Can existing users currently access all of this information?
2. Does each of these roles truly need access to all areas of available information?
3. Are the users unable to carry out the requirements of their job if they do not have access to this information?
4. Can harm be caused to the patient if the user does not have access to this information?
5. Are there professional practice standards requiring the user to have access to this information?
6. Is the information required to support the care of the patient across the continuum of care?
7. Does the individual request regular and routine access to this information or does he or she only require access on an occasional basis where other methods of access may suffice?

To be effective as a privacy-enhancing mechanism, roles-based access should be used in conjunction with additional privacy and security controls such as the following:

1. Unique user IDs and passwords to access the EMR system.
2. Not granting access until the user is authorized by a physician, has completed training, is provided with privacy education, has signed a confidentiality agreement, and is made aware of office privacy and confidentiality policies.
3. Ensuring that audit log capability is activated in the EMR to capture all user access to patient information for the purposes of compliance monitoring and incident investigation.
4. Managing user accounts including adding, modifying, and de-activating user accounts on a regular and timely basis.

Due to physicians' responsibilities for data stewardship, it is important to note that physicians assume responsibility for the accesses made to patient information, including access by staff and delegates.

Consent and Disclosure Directives in BC

This section will:
• Define physician responsibilities regarding patient implied and expressed consent. • Define disclosure directives and their implementation in BC.

Under the BC Personal Information Protection Act (PIPA), consent for collection, use, and disclosure of personal information for direct health care purposes in the province operates primarily on an implied consent model. Individuals who form part of a patient's "circle of care" (e.g., specialists, referring physicians, lab technologists) can access, use, disclose, and retain patient information for the purposes of ongoing care and treatment.

Implied consent must be informed, and physicians should provide adequate information to patients on how they manage the privacy of patient information (see the section Ten Steps to Help Physicians Comply with PIPA and the handout Privacy of Your Personal Health Information). Implied consent is signified by the acceptance by a reasonable individual for the collection, use, and disclosure of information for an obvious purpose where it is understood that the individual will indicate if he or she does not accept ("opt-out" model). For implied consent to be meaningful, the individual has to know that he or she has the right to expressly withhold or withdraw consent at any time without fear of retribution.

Expressed consent from a patient is required when identifiable personal information is intended to be collected, used, or disclosed outside of the circle of care or for secondary purposes such as research (see the section Secondary Use of Personal Information for Research). Expressed consent is signified by the willing agreement of an individual for the collection, use, and disclosure of personal information for a defined purpose ("opt-in" model). The consent can be given verbally or in writing.

Consent is **not** required in circumstances permitted or required by law, such as:

- Statutory duty to report
- Court order
- Coroners investigation
- College investigation.

Disclosure Directives in the Provincial Electronic Health Record (EHR)

Under the provincial e-Health Act (see the section Privacy and Security in the BC Health Care System Today) the Minister of Health must, in a designation order for a provincial health information bank (HIB), authorize the making of disclosure directives by a person whose personal health information is stored in the HIB—one of several data repositories underlying the EHR.

Disclosure directives are optional statements made by an individual or his or her authorized personal representative that request all or portions of personal health information in his or her EHR be "masked" so that it cannot be disclosed without the individual's expressed consent. This expressed consent must be provided to an authorized user with the appropriate permissions to access the information with consent. A disclosure directive remains in effect until it is revoked in writing by the individual who created it. As there is no choice to opt in or consent to the personal information being uploaded to an HIB, disclosure directives provide individuals with the ability to restrict access to their information. Disclosure directives can be overridden in an emergency by authorized users who have the permission to do so, and where the individual is unable to give consent. The override is recorded in an audit trail and is expected to generate an alert for follow-up by an individual responsible for privacy compliance.

It is important to note that disclosure directives legally apply only to HIBs as specified in the designation order under the provincial e-Health Act. The idea of masking sensitive health information, however, is a feature that many Electronic Medical Record (EMR) applications have explored and implemented at varying levels. The ability to mask and unmask personal information in the EMR is often considered when a single EMR application is shared in a group practice setting. This provides patients with the ability to control who in the group practice may or may not have access to portions or all of their personal information.

Physicians should inform patients of the risks related to placing disclosure directives or masking on their record. If a competent patient decides to maintain the disclosure directives, physicians must:

- Honor the patient's decision.
- Document in the patient's medical record the discussion and the patient's decision.
- Provide the best care possible working with the information at their disposal.

For a physician who is treating a patient, whether or not the disclosure directive is in place, the obligation to obtain a proper history from the patients remains. Taking a proper history may elicit relevant information, even if that information is the subject of the disclosure directive. To the extent that it is apparent that a patient refuses to discuss relevant information, this refusal should also be adequately documented.

Additional Privacy Resources for Physicians

BC Privacy Legislation:

BC e-Health Act News Release

Freedom of Information and Protection of Privacy Act (FIPPA)

Personal Information Protection Act (PIPA)

Data Stewardship and Data Sharing:

BC College of Physicians and Surgeons: Data Stewardship Framework

Canadian Medical Association: Data Stewardship: Working Principles

Canadian Medical Protective Association Data Sharing Principles for EMR/EHR

Office of the Information and Privacy Commissioners

- **for BC:** www.oipc.bc.ca
- **for Canada:** www.privcom.gc.ca
- **for Ontario:** www.ipc.on.ca

Privacy Codes, Ethics, Principles:

Canadian Medical Association Code of Ethics

Health information privacy code

Canadian Medical Association: Protection of Health Information

Plain language guide for physicians to CMA health information privacy code

Plain language summary (CMA health information privacy code)

Privacy Toolkits:

Canadian Medical Association Privacy Wizard

Ontario Physician Privacy Toolkit

Other Resources for Physicians/Practitioners:

BC Ministry of Management Services: PIPA Implementation Tools

COACH Guidelines for the Protection of Health Information 2007

Electronic Health Information and Privacy Survey: What Canadians Think

Key Steps for Physicians in Responding to Privacy Breaches

Medical Records in Private Physician Offices

Physician-Patient E-mail Communication: Legal Risks Information Letter

Physicians and Security of Personal Information

Privacy in Practice: A Handbook for Canadian Physicians

Definitions

Access
The process of viewing and/or obtaining data and/or personal information.

Application Service Provider (ASP)
A company that manages and stores the Electronic Medical Record (EMR) at its data centre, rather than the physician managing and running servers in his or her own office. The EMR is then accessed over the Internet or preferably over a private network.

Authentication
A method designed to allow a computer application to provide credentials—usually in the form of a user name and password.

Canadian Medical Association (CMA) Privacy Wizard
An online tool developed by the CMA and all the provincial medical associations that helps physicians ensure they have met key privacy requirements.

Circle of Care
A principle that recognizes and understands the practicality of the need for implied consent for relevant information to flow from one health care provider to another in order to ensure the best level of patient care, unless the health care provider who provides the information is aware that the individual has expressly withheld or withdrawn consent. This is an evolving concept that recognizes the unique challenges for obtaining informational consent in the health care environment.

The definitions around the circle of care relate to the care and treatment of the patient and health care services for the therapeutic benefit of the patient. This includes diagnostic information and professional case consultation with other health care providers. The health care providers within the circle of care should be obvious to the patient and reflect common practices.

Collection
The gathering, acquisition, receipt, or obtaining of personal information.

Confidentiality
The ethical principle or legal right that a physician or other health professional will hold secret all information relating to a patient, unless the patient gives consent permitting disclosure.

Consent
See **Implied Consent** and **Expressed Consent**.

Data Stewardship
The management of personal health information including the collection, use, access, disclosure and retention, and the legal, ethical, and fiduciary responsibilities of a physician in such management.

Disclosure
Making information available to another organization or third party, or to the individual the information is about.

Disclosure Directives
An individual's ability to control when and by whom his or her personal health information will be accessed.

e-Health Act
Legislation that was introduced in 2008 to provide a privacy framework for governing personal information in databanks designated by the Minister of Health as Health Information Banks (HIBs). Also known as the Personal Health Information Access and Protection of Privacy Act, or Bill 24.

Electronic
A format of data storage that includes digital, voice, video, etc.

Electronic Health Record (EHR)
In BC, an electronic record that is patient-centric and contains information from a broad range of health providers. It generally contains a subset of sharable information including cumulative patient profiles with current prescriptions, allergies, and immunization history. It may have integrated information related to in-patient and out-patient encounters with the health care system. Information in the EHR is not always accessed with each patient encounter, but is used when additional information is required during a patient visit. Laboratory, diagnostic imaging results, and other reports are also found in the EHR but are not necessarily delivered to a specific provider for review (e.g., information is reviewed on the part of the provider at the time the information is required).

Electronic Medical Record (EMR)
In BC, a medical record that is in a digital format and is provider-centric. It focuses on medical or physician-specific information and is configured to reflect the needs of individual physicians or groups of physicians responsible for the direct care of a patient.

Electronic Medical Record (EMR) vendor
A company that sells and supports Electronic Medical Record (EMR) software.

Encryption
The conversion of data into an electronic form that cannot be easily understood by unauthorized users.

Expressed Consent
Consent signified by the willing agreement of an individual for the collection, use, and disclosure of personal information for a defined purpose (opt-in model). The consent can be given verbally or in writing. (*See also* **Implied Consent**.)

Freedom of Information and Protection of Privacy Act (FIPPA)
BC legislation that governs personal information collected, used, and disclosed by public bodies including Health Authorities and the Ministry of Health Services.

Handheld Device
Any mobile handheld device that provides computing and information storage and retrieval capabilities for personal or business use (e.g., Blackberry). Such devices are frequently used to maintain an electronic schedule or contact information.

Health Information Bank (HIB)
In general, an electronic database that allows consumers of health services to collect, store, control, and share health information with members in their circle of care. In BC, since the e-Health Act came into effect into 2008, organizations have to apply to be certified as an HIB and are subject to a number of legislated expectations.

Implied Consent
Consent signified by the acceptance by a reasonable individual for the collection, use, and disclosure of information for an obvious purpose where it is understood that the individual will indicate if he or she does not accept (opt-out model). For implied consent to be meaningful, the individual has to know that he or she has the right to expressly withhold or withdraw consent at any time without fear of retribution. (*See also* **Expressed Consent**.)

Individual
The person/patient about whom information is collected. This includes persons who are authorized to exercise rights on behalf of an individual/patient (e.g., parents on behalf of a child; guardian or trustee; personal representative).

Information-Sharing Agreement (ISA)
A formal agreement between organizations and other persons or bodies acting on behalf of the organization that define specific uses and disclosures for shared data. The agreement should include who is permitted to access the data, disclosures for which the data will be used, and conditions and limitations on the collection, use, disclosure of the information.

Masking
The application of rules that restrict access to data in an electronic record, unless additional action is taken to override the restriction. This is differentiated from "blocking," which is an application of access restriction where the existence of the data is not presented. Masking can be applied at different levels depending on the unique circumstance and system capabilities.

Need to know principle
Access to personal information based on a legitimate relationship with the patient and a need to access or use the personal information for the execution of one's duties.

Personal Health Information
Information about an individual that identifies the individual and the individual's health history including physical or mental health; the provision of health services that individual; the registration of the individual for the provision of health services; payments or eligibility for health care; and any information collected in the course of the provision of health services to the individual.

Personal Information
Information, including personal health information, about an identifiable individual which includes factual or subjective information about that individual. This information includes, but is not limited to, name, birth date, physical description, medical history, gender, address, education, employment, and visual images such as photographs or videotapes.

Personal Information Protection Act (PIPA)
BC legislation that governs personal information collected, used, and disclosed by all private sector organizations, including physicians' private practices and other private health care facilities.

Personal Information Protection and Electronic Documents Act (PIPEDA)
The federal legislation that governs the collection, use, and disclosure of personal information by federally regulated private sector organizations.

Privacy
The right to be free from intrusion and interruption. It is linked with other fundamental rights such as freedom and personal autonomy. In relation to information, privacy involves the right of individuals to determine when, how, and to what extent they share information about themselves with others.

Privacy Breach
Unauthorized access to, or the collection, use, disclosure, retention, or destruction of personal health information.

Privacy Impact Assessment (PIA)
A foundation tool/process within FIPPA designed to ensure public organizations' compliance with privacy protection legislation. Can also refer to a structured process of assessing the privacy and security aspects of a given process or project.

Privacy Officer
The individual designated with the accountability to ensure organizational compliance with privacy legislation, industry standards, and professional and regulatory obligations. The Privacy Officer is responsible for policy development, compliance monitoring, privacy breach management, staff training, and managing complaints, questions and access to personal information requests. In a medical practice, it is recommended that the Privacy Officer be a physician. This means that if the office is a solo practice, the solo physician is the *de facto* Privacy Officer. In a group practice, one of the physicians must be identified as being responsible for this function.

Private Network
A secure, private, end-to-end network (patient data does not travel over the Internet) that allows secure, high-speed access to an EMR or an EHR, secure Internet access, and secure email messaging.

Private Physician Network (PPN)
A secure, private, end-to-end network (patient data does not travel over the Internet) provided by the BC government to BC physicians to enable greater security and rapidity for the PITO ASP based EMRs. The PPN allows secure, high-speed access to the PITO EMRs and secure email messaging.

Reasonableness of Security Measures
As described in a 2006 report of the BC Information and Privacy Commissioner, "the measure by which security measures are objectively diligent and prudent in the circumstance." The report also stated that "what is 'reasonable' may signify a very high level of rigour depending on the situation."

Remote Access
The ability to get access to a computer or network from a remote distance. Individuals who are travelling or working from home may need access to information, and may access the network and systems remotely.

Roles-Based Access
A policy and technical architecture involving the assignment of access privileges to roles rather than to individual users. Users are granted privileges by virtue of being authorized to act in specific roles.

Security
The preservation of the confidentiality, integrity, and availability of personal information. It is achieved by implementing policies and procedures based on relevant legislation, industry standards, design and implementation of appropriate technology solutions, and managing ongoing operations relating to access to personal information.

Third Party
In the context of sharing personal information, any person, group of persons, or organization other than the person or organization who directly collected the personal information.

Staff
For the purposes of this document, locum physicians, associates, visiting specialists, medical students, residents, physicians-in-training, contractors, and volunteers with whom you collect, use, or disclose personal information.

Strong Password
A password that is sufficiently long, random, or otherwise producible only by the user who creates it. It is case sensitive and includes a random combination of alphanumerics and symbols. The College recommends that a strong password should be eight or more characters in length and contain at least one number, one letter, and one symbol (e.g., Brown#123).

Two Factor Authentication
The combination of user name/password and some other physical identification tool (e.g., secure ID token in order to verify the identity of a person).

Use
The application of information for a specific purpose by the person or organization that collected the information.

USB Memory Key
A compact data storage device that is typically removable and rewriteable. The most common use of USB memory keys are to transport and store files such as documents, pictures, and videos.

Virtual Private Network (VPN)
An authentication and encryption mechanism that allows connection from outside the physician's office to the EMR over the Internet with enhanced security.

Wireless
The transfer of information over a distance without the use of electrical conductors or wires.

Privacy and Security Checklist

A. Clinic Policies and Procedures	Y	N	Comments
1. Do you have an office privacy policy that deals with confidentiality of personal health information including printing, transfer, storage, and secure disposal of patient records?	☐	☐	
2. Are procedures in place for dealing with actual and suspected privacy and security incidents and breach investigations?	☐	☐	
3. Are processes in place to securely dispose of paper documents and old electronic devices (such as data storage, computers, etc.) that may contain confidential data?	☐	☐	

B. Staff	Y	N	Comments
4. Have you appointed an individual (and delegate) responsible for privacy and security? This person would be responsible for answering questions (e.g., from patients), but also responding to complaints, incidents, breaches, audits, and making sure that staff are trained and policies/procedures are up-to-date.	☐	☐	
5. Have staff members signed a confidentiality agreement?	☐	☐	
6. Have staff members been trained about how to maintain privacy and confidentially of personal health information?	☐	☐	
7. Do you have ongoing annual privacy and security awareness training that includes how users must safeguard their user IDs and passwords, keys, tokens, and other access credentials?	☐	☐	

C. Partners	Y	N	Comments
8. Do contracts with third parties (e.g., paper-shredding service) include privacy and confidentiality clauses?	☐	☐	

D. Patients	Y	N	Comments
9. Is a patient privacy notice or other communication materials that inform patient about privacy and information practices available?	☐	☐	
10. Are procedures available for dealing with patient requests for information, corrections, and complaints?	☐	☐	

Additional considerations, if using computers, faxes, and electronic devices

E. EMR and Business Continuity Copy (BCC)	Y	N	Comments
11. Have you appointed an individual responsible for ongoing EMR user account management (new user set-up, changes to user privileges, de-activation of old user accounts)?	☐	☐	
12. Has a unique user ID and strong password been assigned to each individual user accessing the EMR?	☐	☐	
13. Have you developed and implemented a roles-based access model?	☐	☐	
14. Has the systems audit trail functionality been enabled?	☐	☐	
15. Do you have an audit schedule and procedures in place for a designated individual to routinely and periodically (i.e., spot-audits) monitor audit trails?	☐	☐	

F. Hardware and peripherals	Y	N	Comments
16. Do your policies address fax and email use?	☐	☐	
17. Are peripheral devices (printers, fax machines) located in secure areas to prevent unauthorized access?	☐	☐	
18. Are computer monitors situated in a manner that prevents unauthorized viewing?	☐	☐	
19. Is any patient data stored on desktop computers, laptops, or mobile storage (e.g., memory keys) encrypted?	☐	☐	
20. Are procedures and technical controls (e.g., application time-out) in place to prevent screens from being viewed if the computer user leaves the computer?	☐	☐	
21. Has up-to-date antivirus protection been installed on workstations and are anti-virus controls always on and enabled?	☐	☐	
22. Are firewalls installed on computers with access to the Internet?	☐	☐	

G. Local Area Network (LAN) and wireless	Y	N	Comments
23. Have appropriate controls been set up to secure the Local Area Network (LAN), if you have one in place?	☐	☐	
24. Have wireless security settings been appropriately configured and enabled (e.g., restrict wireless transmission, firewalls, encryption is used, etc.), if they are in place?	☐	☐	
25. Have appropriate controls been set up to secure the Virtual Private Network (VPN), if you have one in place?	☐	☐	

Sample office privacy policy (*from CMA Privacy Wizard*)

Dr. Joe Smith, Family Physician
222 Smith Way, SmithFalls, ON
222-2222; Jsmith@email; Dr.Smith/mydoctor.ca

Protecting Personal Information

1. Openness and transparency

1.1 We value patient privacy and act to ensure that it is protected.

1.2 This policy was written to capture our current practices and to respond to federal and provincial requirements for the protection of personal information.

1.3 This policy describes how this office collects, protects and discloses the personal information of patients and the rights of patients with respect to their personal information.

1.4 We are available to answer any patient questions regarding our privacy practices.

2. Accountability

2.1 The physician is ultimately accountable for the protection of the health records in his/her possession.

2.2 Patient information is sensitive by nature. Employees and all others in this office who assist with or provide care (including students and locums) are required to be aware of and adhere to the protections described in this policy for the appropriate use and disclosure of personal information.

2.3 All persons in this office who have access to personal information must adhere to the following information management practices

- ☐ Office information management practices
  - ☐ Access is on a need to know basis
  - ☐ Access is restricted to authorized users
- ☐ third party obligations
  - ☐ contractual privacy clauses/agreements with third parties (including cleaning and security personnel, landlords, data processors, etc)

2.4 This office employs strict privacy protections to ensure that

- ☐ We protect the confidentiality of any personal information we access in the course of providing patient care.
- ☐ We collect, use and disclose personal information only for the purposes of providing care and treatment or the administration of that care, or for other purposes expressly consented to by the patient.
- ☐ We adhere to the privacy and security policies and procedures of this office.
- ☐ We educate and train staff on the importance of protecting personal information.

Collection, Use and Disclosure of Personal Information

3. Collection of personal information

3.1 We collect the following personal information

- ☐ Identification/Contact information, including
  - ☐ name
  - ☐ date of birth
- ☐ Billing information, including
  - ☐ Provincial/territorial health insurance plan (health card) number
  - ☐ private medical insurance details
- ☐ Health information, which may include
  - ☐ medical history
  - ☐ presenting symptoms

3.2 Limits on collection

We will only collect the information that is required to provide care, administrate the care that is provided, and communicate with patients. We will not collect any other information, or allow information to be used for other purposes, without the patient's express consent - except where authorized to do so by law. These limits on collection ensure that we do not collect unnecessary information.

4. Use of personal information

4.1 Personal information collected from patients is used by this office for the purposes of

- ☐ Identification and contact
  - ☐ emergency contact
- ☐ Provision and continuity of care
  - ☐ Historical record
  - ☐ Health promotion and prevention
- ☐ Administrate the care that is provided
  - ☐ Prioritization of appointment scheduling
  - ☐ Billing provincial health plan
- ☐ Professional requirements
  - ☐ Risk or error management, i.e., medical-legal advice (CMPA)
  - ☐ Quality assurance (peer review)
- ☐ Research studies and trials

5. Disclosure of personal information

5.1 Implied consent (Disclosures to other providers)

5.1.1 Unless otherwise indicated, you can assume that patients have consented to the use of their information for the purposes of providing them with care, including sharing the information with other health providers involved in their care. By virtue of seeking care from us, the patient's consent is implied for the provision of that care.

5.1.2 Relevant health information is shared with other providers involved in the patient's care, including (but not limited to)

- ☐ other physicians in this practice
- ☐ other physicians in the after hours call group

5.2 Without consent (Disclosures mandated or authorized by law)

5.2.1 There are limited situations where the physician is legally required to disclose personal information without the patient's consent. Examples of these situations include (but are not limited to)

- ☐ billing provincial health plans
- ☐ reporting specific diseases
- ☐ reporting abuse (child, elder, spouse, etc)
- ☐ reporting fitness (to drive, fly, etc)
- ☐ by court order (when subpoenaed in a court case)
- ☐ in regulatory investigations
- ☐ for quality assessment (peer review)
- ☐ for risk and error management, e.g., medical-legal advice

5.3 Express Consent (Disclosures to all other third parties)

5.3.1 The patient's express consent (oral or written) is required before we will disclose personal information to third parties for any purpose other than to provide care or unless authorized to do so by law.

5.3.2 Examples of situations that involve disclosures to third parties include (but are not limited to)

- ☐ third party medical examinations
- ☐ provision of charts or chart summaries to insurance companies

5.3.3 Disclosure Log

Before a disclosure is made to a third party, a notation shall be made in the file that the patient has provided express consent, or a signed patient consent form is appended to the file.

5.4 Withdrawal of consent

5.4.1 Patients have the option to withdraw consent to have their information shared with other health providers at any time.

5.4.2 Patients also have the option to withdraw consent to have their information shared with third parties.

5.4.3 If a patient chooses to withdraw their consent, the physician will discuss any significant consequences that might result with respect to their care and treatment (e.g., possible negative impact on the care provided).

Office Safeguards

6. Security measures

6.1 Safeguards are in place to protect the security of patient information.

6.2 These safeguards include a combination of physical, technological (for offices where computers are in use) and administrative security measures.

6.2.1 We use the following **physical safeguards**

- ☐ limited access to office
  - ☐ monitored alarm system
  - ☐ deadbolt entry lock (or key card/key pad entry system
- ☐ limited access to records
  - ☐ need to know basis
  - ☐ locked file cabinets
- ☐ office layout/features
  - ☐ front desk privacy screens

☐ soundproofing and/or white noise to ensure confidentiality

6.2.2 We use the following **technological safeguards**

☐ protected computer access for patient health information

- ☐ passwords
- ☐ user authentication

☐ system protections

- ☐ firewall software
- ☐ virus scanning software

☐ Protected external electronic communications - Internet

- ☐ separate internet access (stand alone, not connected to operating system)
- ☐ encrypted email for any external communication of patient health information

☐ secure electronic record disposal

- ☐ safely dispose of computer hard drives
- ☐ destroy all other removable media (diskettes, CD-R, DVD)

Wireless and mobile communication devices (e.g., laptops, PDAs, etc) are especially vulnerable to loss, theft and unauthorized access. We take extra precautions when using these devices for patient health information.

6.2.3 We use the following **administrative safeguards**

☐ Office information management practices

- ☐ Access is on a need to know basis
- ☐ Access is restricted to authorized users

☐ third party obligations

- ☐ contractual privacy clauses/agreements with third parties (including cleaning and security personnel, landlords, data processors, etc)

6.2.3.1 Limits on third party access

Any other persons having access to patient information or to these premises (e.g., cleaners, security staff, landlords) shall, through contractual or other means, provide a comparable level of protection.

6.2.3.2 Staff signed confidentiality agreements

- ☐ We also ensure that all staff have signed confidentiality agreements or clause as part of (or appended to) their employment contract.
- ☐ This confidentiality agreement or clause extends beyond the term of employment.

7. Communications policy

7.1 We are sensitive to the privacy of personal information and this is reflected in how we communicate with our patients, others involved in their care and all third parties.

7.2 We protect personal information regardless of the format.

7.3 We use specific procedures to communicate personal information by

7.3.1 **Telephone**

- ☐ Patient preference with regards to phone messages will be taken into consideration
- ☐ Unless authorized, we only leave our name and phone number on message for patients

7.3.2 **Fax**

- ☐ our fax machine is located in a secure or supervised area (restricted public access)
- ☐ we use of pre-programmed numbers to ensure fax received by proper recipient

7.3.3 **Email**

- ☐ any confidential information sent over public or external networks is encrypted
- ☐ firewall and virus scanning software is in place to mitigate against unauthorized modification, loss, access or disclosure

7.3.4 **Post/Courier**

- ☐ sealed envelope
- ☐ marked confidential

8. Record retention

8.1 We retain patient records as required by law and professional regulations (please refer to your College guidelines).

8.2 The Canadian Medical Protective Association (CMPA) advises members to retain their medical records for at least 10 years from the date of last entry or, in the case of minors, 10 years from the time the patient would have reached the age of majority (age 18 or 19 in all jurisdictions).

8.3 We use secure offsite record storage (locked, fireproof , etc)

8.4 Some colleges advise physicians that claims may arise beyond the stipulated regulatory period, and therefore may want to keep their records longer, particularly if they are aware of a potential claim.

9. Procedures for secure disposal/destruction of personal information

9.1 When information is no longer required, it is destroyed according to set procedures that govern the storage and destruction of personal information (please refer to your College guidelines).

9.1.1 We use the following methods to destroy/dispose of paper records

- ☐ According to provincial/territorial college regulations
- ☐ shredding

9.1.2 We use the following methods to destroy/dispose of electronic records
We seek expert advice on how to dispose of electronic records and hardware. At a minimum, we ensure that all information is wiped clean where possible prior to disposal of electronic data storage devices (e.g., surplus computers, internal and external hard drives, diskettes, tapes, CD-ROMs, etc.)

- ☐ properly disposed of computer hard drive
- ☐ destroy all other electronic media storage (diskettes, CD-R, DVD)

9.2 Disposal log
Before the secure disposal of a health record, we maintain a log with the patient's name, the time period covered by the destroyed record, the method of destruction and the person responsible for supervising the destruction (if applicable).

Patient Rights

10. Access to information

10.1 Patients have the right to access their record in a timely manner.

10.2 If a patient requests a copy of their records, one will be provided at a reasonable cost (please refer to your College guidelines for non-insured services).

10.3 Access shall only be provided upon approval of the physician.

10.4 If the patient wishes to view the original record, one of our staff must be present to maintain the integrity of the record, and a reasonable fee may be charged for this access.

10.5 Patients can submit access requests

- ☐ verbally
- ☐ in writing

10.6 This office follows specific procedures to respond to access requests

- ☐ we acknowledge receipt of request
- ☐ we respond within
  - ☐ a timely fashion
  - ☐ 30 days

11. Limitations on access

11.1 In extremely limited circumstances the patient may be denied access to their records, but only if providing access would create a risk to that patient or to another person.

11.1.1 For example, when the information could reasonably be expected to seriously endanger the mental or physical health or safety of the individual making the request or another person.

11.1.2 Or if the disclosure would reveal personal information about another person who has not consented to the disclosure. In this case, we will do our best to separate out this information and disclose only what is appropriate.

12. Accuracy of information

12.1 We make every effort to ensure that all patient information is recorded accurately.

12.2 If an inaccuracy is noted, the patient can request changes in their own record, and this request is documented by an annotation in the record.

12.3 No notation shall be made without the approval or authorization of the physician.

13. Privacy Complaints

13.1 It is important to us that our privacy policies and practices address patient concerns and respond to patient needs.

13.2 A patient who believes that this office has not responded to their access request or handled their personal information in a reasonable manner is encouraged to address their concerns first with their doctor.

13.2.1 Patient complaints can be made

- ☐ verbally
- ☐ in writing

13.2.2 This office follows specific procedures for responding to patient complaints

- ☐ Our complaints process is readily accessible, transparent and simple to use
- ☐ Patients are informed of relevant complaint mechanisms

13.3 Patients who wish to pursue the matter further are advised to direct their complaints to

- ☐ provincial/territorial college
- ☐ provincial/territorial privacy commissioner

Physician Signature: _____

Date: _____

Sample office privacy handout (*from CMA Privacy Wizard*)

Dr. Joe Smith, Family Physician
222 Smith Way, SmithFalls, ON
222-2222; Jsmith@email; www.mydoctor.ca/drsmith

This policy outlines how we protect the privacy of your personal information and medical record. Everyone working for this office is required to adhere to the protections described in this policy. If you have any questions regarding our privacy practices, please contact your doctor or one of our staff.

Collection, Use and Disclosure of Personal Information

What personal information do we collect?

We collect the following personal information:

- ☐ **Identification** and **Contact** information (name, address, date of birth, emergency contact, etc)
- ☐ **Billing** information (provincial plan and/or private insurer)
- ☐ **Health** information (symptoms, diagnosis, medical history, test results, reports and treatment, record of allergies, prescriptions, etc)

Limits on collection

We collect only the information that is required to provide care, administrate the care that is provided, and communicate with you. We do not collect any other information, or allow information to be used for other purposes, without your express (i.e., verbal or written) consent - except where authorized to do so by law.

When and to whom do we disclose personal information?

Implied consent for provision of care: By virtue of seeking care from us, your consent is implied (i.e., assumed) for your information to be used by this office to provide you with care, and to share with other providers involved in your care.

Disclosure to other health care providers: Relevant health information is shared with other providers involved in your care, including (but not limited to) other physicians and specialists, pharmacists, lab technicians, nutritionists, physiotherapists and occupational therapists.

Disclosures authorized by law: There are limited situations where we are legally required to disclose your personal information without your consent. These situations include (but are not limited to) billing provincial health plans, reporting infectious diseases and fitness to drive, or by court order.

Disclosures to all other parties: Your express consent is required before we will disclose your information to third parties for any purpose other than to provide you with care or unless we are authorized to do so by law. Examples of disclosures to other parties requiring your express consent include (but are not limited to) third party medical examinations, enrolment in clinical (research) trials and provision of charts or chart summaries to insurance companies.

Can you withdraw consent?

You can withdraw your consent to have your information shared other health care providers or other parties at any time, except where the disclosure is authorized by law. However, please discuss this with your physician first.

Patient Rights

How do you access the personal information held by this office?

You have the right to access your record in a timely manner. If you request a copy of your record, one will be provided to you at a reasonable cost. If you wish to view the original record, one of our staff must be present to maintain the integrity of the record, and a reasonable fee may be charged for this access. Patient requests for access to the medical record can be made verbally or in writing to myself or my staff (see office address at top of Policy).

Limitations on access

In extremely limited circumstances you may be denied access to your records, but only if providing access would create a significant risk to you or to another person.

What if you feel your record is not accurate?

We make every effort to ensure that all of your information is recorded accurately. If an inaccuracy is identified, you can request that a note be made to reflect this on your file.

Office Safeguards

How secure is your information?
Safeguards are in place to protect the security of your information. These safeguards include a combination of physical, technological and administrative security measures that are appropriate to the sensitivity of the information. These safeguards are aimed at protecting personal information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification.

What is our communications policy?
We protect personal information regardless of the format. Specific procedures are in place for communicating by phone, email, fax, and post/courier.

How long do we keep information?
We retain patient records as required by law and professional regulations.

How do we dispose of information when it is no longer required?
When information is no longer required, it is destroyed in a secure manner, according to set procedures that govern the storage and destruction of personal information.

Complaints process

If you believe that this office has not replied to your access request or has not handled your personal information in a reasonable manner, please address your concerns first with your doctor.

Your may also choose to make a complaint to
- relevant licensing authority
- provincial privacy commissioner
- federal privacy commissioner

(Physician) Signature: _____

Date: _____

This policy was created with the help of the CMA PRIVACYWIZARD™

Patient Request for Access to Personal Information

Upon request, we will give a patient (or the patient's legally authorized representative) access to his or her personal information from the records we have in our custody or that are under our control. Our designated privacy officer will also explain how we collect and use personal information, and to whom it has been disclosed.

Within 30 working days of receiving your completed request for access to personal information (see attached form), we will provide you with a copy of the information, let you review the original records if we cannot reasonably provide copies to you, or give reasons for not providing access. We may extend the time for responding to your request in certain circumstances. We may also be permitted or required by law to refuse to give you access to some information in your records.

If we refuse access, our Privacy Officer will explain the reasons for this. If you disagree with our decision, we will try to resolve the matter with you. If we cannot resolve the matter to your satisfaction, you may ask the College of Physicians and Surgeons of BC to try to resolve it. If you are still not satisfied, you may refer the matter to the Office of the Information and Privacy Commissioner for BC (OIPC) .

BC's Personal Information Protection Act allows us to charge you a minimal fee for access to your personal information. If a fee is to be charged, we will provide you with a written estimate before we provide the service. We may require you to pay a deposit for all or part of the fee before we provide the service.

PATIENT REQUEST FORM FOR ACCESS TO PERSONAL INFORMATION

The information on this form will be used to respond to your request for your personal information or the personal information of someone whom you are legally entitled to represent.

Whose information do you want access to?

- ☐ My own personal information
- ☐ Another person's personal information

Please complete the "Patient Information" and "Authorized Representative's Contact Information" sections below, and attach proof that you can legally act on behalf of that individual.

Patient information

Mr / Mrs / Ms (please circle)

Last name: _____

First name: _____

Personal health number: _____

Date of birth (dd/mm/yy): _____

Street address: _____

City/town: _____ Prov. ____

Postal code: _____ Fax_____

Tel: (home) _____ (bus) _____

Email address: _____

Please describe, in as much detail as possible, the information you want to access. Indicate if you also want access to records about the disclosure of your information, or information of the person you are representing. Be sure to give previous names, if any.

_____

_____

_____

_____

_____

Please indicate if you wish to:

- ☐ Receive a photocopy of the record.
  Please note that a base fee of $_____ per page applies for each page copied. For convenience, you may enclose this fee with your request. You will be provided with an estimate of any additional costs.
- ☐ View the original record, without receiving a copy.
  Please ask for an estimate of the fee you will be charged for:
  - ☐ Review of the original by the physician ***and / or***

☐ Supervision by physician or designated staff person for your review
A deposit of 50% of the fee may be required.

_____ _____
Patient Signature Date (dd/mm/yy)

Access by authorized representative

I am a legally authorized representative of the patient named above and have attached proof of that representation. I hereby request access to the patient's personal records on his or her behalf.

Authorized representative's contact information

Mr / Mrs / Ms (please circle) Street address: _____
Last name: _____ City/town: _____ Prov. _____
First name: _____ Postal code: _____ _____
Telephone (home): _____ Telephone (business) _____
Fax: _____ Email address: _____

_____ _____
Authorized Representative's Signature Date (dd/mm/yy)

Patient Request for Correction to Personal Information

If you believe your patient records with our office are inaccurate or incomplete, you (or your legally authorized representative) may ask us to correct the error or omission. Our Privacy Officer or staff member will explain the process.

Within 30 working days of receiving your completed request for correction to personal information (see attached form), we will correct or amend any information in your patient record that we have verified to be inaccurate or incomplete, then send a copy of the corrected record to each organization to which the inaccurate or incomplete information was disclosed within the past year.

If we decide that no correction is necessary, our Privacy Officer will explain the reasons for this. We will not correct or change an opinion, including a professional or expert opinion. We will note your requested correction and reasons for not making any correction and include it in your record, to indicate a correction was requested but not made.

If you disagree and believe that a change should have been made, we will attempt to resolve the matter with you. If we cannot resolve the matter, we will tell you how to request a review by the College of Physicians and Surgeons of BC. If you are still unsatisfied after that review, you may take the matter to the Office of the Information and Privacy Commissioner for BC (OIPC) .

To request a correction to your personal information, please complete the attached form. If you need assistance, our Privacy Officer will help you complete the form.

REQUEST FORM TO CORRECT OR AMEND PERSONAL INFORMATION

The information gathered on this form will be used to respond to your request for a correction to your personal information or the personal information of someone you are legally entitled to represent.

Whose information do you want to correct?

- ☐ My own personal information
- ☐ Another person's personal information

Please complete the "Patient Information" and "Authorized Representative's Contact Information" sections below, and attach proof that you can legally act on behalf of that individual.

Patient information

Mr / Mrs / Ms (please circle)

Last name: _____

First name: _____

Personal health number: _____

Date of birth (dd/mm/yy): _____

Street address: _____

City/town: _____ Prov. ____

Postal code: _____ Fax_____

Tel: (home) _____ (bus) _____

Email address: _____

Please describe, in as much detail as you can, the information you want corrected. Be sure to give the complete patient name that is in the records if it is different from the name given above. If you need more space, please attach a separate sheet of paper.

_____

_____

_____

_____

_____

What correction or amendment do you want to make and why? Please attach any documents that support your request.

_____

_____

_____

_____

_____

_____ _____

Patient Signature Date (dd/mm/yy)

Corrections by authorized representative

I am a legally authorized representative of the patient named above and have attached proof of that representation. I hereby request a correction to the patient's personal records on his or her behalf.

Authorized representative's contact information

Mr / Mrs / Ms (please circle) Street address: _____

Last name: _____ City/town: _____ Prov. _____

First name: _____ Postal code: _____ _____

Telephone (home): _____ Telephone (business) _____

Fax: _____ Email address: _____

_____ _____

Authorized Representative's Signature Date (dd/mm/yy)

Confidentiality Agreement for Physician Office Employees

The BC Personal Information Protection Act (PIPA) legally governs personal information collected, used, stored, and disclosed by this medical practice. As such, you are required to acknowledge each term of this agreement:

- I am aware that personal information of both patients and employees that is collected, used, stored, and disclosed, that comes to my attention as a result of my employment with this medical practice, must be kept confidential and secure as per PIPA and the office's policies, both during and after my term of employment.

- I understand and agree that it is my responsibility to be familiar with the practice's policies and procedures regarding privacy, confidentiality and security of personal information and that I am expected to comply.

- I will access and use personal information of patients only on a "need to know" basis as it pertains to my role and responsibilities.

- I will only share personal information with individuals who need to know and who are also involved in providing health care services to the patient.

- I will strive to keep patient personal information accurate and up-to-date.

- I understand that I cannot access my own personal information or that of family, friends, or co-workers unless they are under my direct care or if I need to do so as part of my official duties and responsibilities with the practice.

- Should I have reason to believe that a privacy breach has occurred, I will notify the individual responsible for privacy in the office.

- I hereby acknowledge that failure to comply with these terms can lead to disciplinary action, which may include termination of access, termination of employment, withdrawal of privileges, termination of contract, and/or professional sanctions.

Employee Print Name: _____

Signature: _____

Date (dd/mm/yyyy): _____

Medical Practice or Physician Print Name: _____

Privacy Officer Witness Print Name: _____

Signature: _____

Date (dd/mm/yyyy): _____

Confidentiality Agreement for Third Parties

The service provider named below hereby agrees that it will not use or disclosure any identifiable patient information (whether received or created before or after the date of this agreement) except for the purposes necessary to perform services for the medical practice named below, as set out in the service contract entered into between the service provider and the medical practice before this date ("service agreement") or with the prior written consent of the medical practice in its sole discretion or as compelled by law.

The service provider represents that it has safeguards in place, equal or superior to the medical practice named below, to protect the security of patient information. The service provider agrees to securely dispose of identifiable patient information once it is no longer required for the purposes specified in the service contract and to notify the medical practice within a reasonable time thereafter that this has been done and how it has been done.

The service provider agrees that there will be no disclosure of personal identifiable information outside of Canada and no access to this information from outside Canada without prior consent from the medical practice.

The service provider represents that it is aware of and fully compliant with BC's Personal Information Protection Act (PIPA) and agrees to comply with that Act. The service provider acknowledges and agrees that any breach of this agreement may result in termination of the service agreement and in penalties envisaged by PIPA.

Service Provider	**Name:** (please print)	_____
Authorized Signatory	**Name:** (please print)	_____
	Signature:	_____
	Date: (dd/mm/yyyy)	_____
Medical Practice or Doctor	**Name:** (please print)	_____
Witness (Privacy Officer)	**Name:**	_____
	Signature:	_____
	Date: (dd/mm/yyyy)	_____

Confidentiality Agreement for Health Authority Employees working within a Physician practice's Premises

I, _____, hereby agree that I will not use or disclose any patient personal information collected, accessed, or otherwise obtained by me at the <Physician Practice> except for the purposes necessary to perform authorized services.

I will abide by the <Physician Practice> privacy policy concerning its records and will protect the privacy and security of patient information including:

1. I will only access files of patients who have consented to do so.

2. I will not collect, use, or disclose patient personal information for any purpose other than the authorized purposes or as permitted or required by law.

3. I will protect patient personal information using appropriate security safeguards, and will allow only authorized individuals who are directly involved to have access to it.

4. I will strive to keep patient personal information accurate and up-to-date.

5. Subject to any Health Authority or physician office policies with regard to retention of health records, I will securely dispose of identifiable patient information that I create once it is no longer required.

I am aware of and will fully comply with the Personal Information Protection Act (PIPA) as directed by Physician Practice policies and the Freedom of Information and Protection of Privacy Act (FIPPA) in respect of records in the custody of control of the <Health Authority Name>. I acknowledge and agree that any breach of this Confidentiality Agreement may result in termination of my services to the Physician Practice and in penalties as envisaged by PIPA and FIPPA.

Health Authority Employee
Name (please print)**:** _____

Signature: _____

Date (dd/mm/yyyy): _____

Witness
Name (please print)**:** _____

Signature: _____

Date (dd/mm/yyyy): _____