BC Physician Privacy Toolkit
A guide for physicians in private practice

3rd Edition

Updated August 2017

WARNING AND DISCLAIMER

This BC Physician Privacy Toolkit has been prepared by the Doctors of BC (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 physicians in complying with the law and meeting the expectations of patients and the public in relation to health privacy. 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 application 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 third edition of the BC Physician Privacy Toolkit. Your feedback is always appreciated. Please contact any of the three organizations with your questions or comments:

- Doctors of BC (BCMA) www.doctorsofbc.ca
- 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

Contents

Legislative Framework for Privacy in the BC Health Care System

This section will:

- summarize the private sector privacy legislation in BC that applies to physicians in private practice and private health care organizations: *Personal Information Protection Act [SBC 2003 c 63] (PIPA)*
- explain the requirements related to patient consent
- summarize the public sector privacy legislation in BC that applies to public bodies, such as health care organizations, health authorities, professional regulatory bodies, ministries and other government agencies:
    - *Freedom of Information and Protection of Privacy Act [RSBC 1996 c 165]. (FIPPA)*
    - *E-Health Act*
- Explain the:
    - difference between PIPA and FIPPA
    - role of the Information and Privacy Commissioner for BC
    - difference between Electronic Medical Records (EMRs) and Electronic Health Records (EHRs)
    - provision of collaborative care and use of EHRs

Privacy in the BC Health Care System

Personal health information is one of the most sensitive types of personal information because it encompasses the physical, mental and emotional status of individuals over their lifetime. It 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 commerce.

Protecting patients' personal health information is a priority for physicians because it is fundamental to maintaining the physician-patient relationship. When seeking medical care, patients disclose their personal health information because they trust their physician to protect their privacy. If patients do not have confidence that their physician has adequate safeguards in place to protect their personal health information, they may 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 Canadian Medical Association (CMA) survey, which found that 11% of the public withheld 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 themselves. The Supreme Court of Canada has validated this concern and recognized it in the *Canadian Charter of Rights and Freedoms*:

- Section 7 includes the right to be free of the psychological stress resulting from the unauthorized disclosure of one's personal health information.
- Section 8 includes the right to be free from unreasonable search and seizure, including where police authorities request information from a physician about a patient without a warrant, subpoena, court order or other legal authority.

Physicians are governed by the professional requirements as set out in the *Health Professions Act*, the College of Physicians and Surgeons of BC Bylaws, relevant professional standards and guidelines of the College of Physicians and Surgeons of BC, and the CMA Code of Ethics.

For physicians who work within public health care organizations such as hospitals, health authorities, and the BC Ministry of Health, the protection of, and individual's access to, personal information is governed by FIPPA, as well as the applicable requirements of the College of Physicians and Surgeons.

Privacy and security in the health care system today must balance two competing social benefits, namely the need to:

- appropriately access and share information to enhance care quality and safety and provide continuity of care
- implement reasonable safeguards to protect personal health information

Balancing these two needs presents challenges 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., role-based access control, auditing, authentication mechanisms, encryption). Implementing these measures will build and maintain public trust and confidence in the privacy and security of personal health information.

Adequately protecting personal health information is a complex undertaking within the context of requirements of privacy legislation, new information technologies (including EMRs and EHRs), new models for information sharing, collaborative teams, and contractual arrangements with service providers. But none of these factors, including the introduction of new information technologies, change the responsibilities of physicians to appropriately protect personal health information; nor do they eliminate the risks to personal health information. Rather, different methods for safeguarding personal health

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 but exceed their authorized limits).

BC's *Personal Information Protection Act* (PIPA)

PIPA applies to private organizations, including physician practices, and governs how personal information about 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 Ministry of Health. Those entities are governed by FIPPA (see below).

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). Personal information includes employee personal information, but not business contact information or work product information.

The core principle of PIPA relevant to physicians is that personal information should not be collected, used, or disclosed without the voluntary and informed "consent" of the individual. This principle is subject to limited exceptions. For example, consent is not required where the collection, use, and disclosure is:

- clearly in the interests of the individual and consent cannot be obtained in a timely way; or
- 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

There are two types of consent: express and implied. Patients provide "express consent" when they agree, verbally or in writing to the collection, use or disclosure of their personal information for a particular purpose. Express consent is necessary for research purposes, education purposes, or other purposes that are not related to the patient's care. "Implied consent" on the other hand is deemed to be given

where the purpose of collection, use, or disclosure would be considered to be obvious to a reasonable person, and where the individual voluntarily provides the information. The collection, use and disclosure of personal information for direct health care purposes in BC is usually authorized by implied consent. Implied consent can also be provided by giving a patient the opportunity to "opt-out" (e.g. when informing the patient about a referral, you provide them with a reasonable time to decline).

Under PIPA, physicians have custody of the personal health information they have collected and physical control of the documents/electronic data. They are accountable for any privacy breach that occurs to personal health information in their custody and control, including any breach committed by an employee under their authority.

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

In BC, public health care bodies such as hospitals, health authorities, and the Ministry of Health are subject to the privacy protective measures contained in FIPPA. FIPPA guarantees the right of individuals to gain access to and request correction of personal information collected about them by public bodies. It also prohibits the unauthorized collection, use, or disclosure of personal information by public bodies and requires that reasonable safeguards be put in place to protect personal information. FIPPA does not apply to personal information collected and stored in a physician's private practice, private laboratories or other private health providers as PIPA governs these organizations (see above).

FIPPA prohibits the disclosure of personal information outside of Canada as well as any access to such records from outside Canada by health authorities and other public bodies without express consent (except in limited circumstances). It also provides whistle-blower protections for individuals who report contraventions of FIPPA in good faith, including unauthorized disclosure and access as well as foreign demands for disclosure or access.

FIPPA permits public bodies to provide "foreign access" under certain circumstances, such as performing system and equipment maintenance or data recovery from out-of-country, or with consent, and subject to other 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 needed to complete the task.

Comparing PIPA and FIPPA

Physicians in private practice who are also providing services to a public health care body will generally be governed by PIPA with respect to the personal information collected, used and disclosed by the

private practice, and by FIPPA with respect to the personal information they collect, use and disclose in their capacity as physicians for the public health care body.

There are some notable differences between PIPA and FIPPA:

- PIPA does not restrict the storage of, or access to personal information from outside Canada. As long as privacy is sufficiently protected, data can be stored or accessed from outside Canada.
- 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 express (written or verbal opt-in) or implied (opt-out or deemed).
- FIPPA does not permit the collection, use and disclosure of personal information on the basis of consent to the same extent as PIPA; instead it operates on the principle of appropriate authority and "notification" for collection of information.

BC's E-Health Act

The BC *E-Health (Personal Health Information Access and Protection of Privacy)* Act was enacted to provide legislative authority and a privacy framework to protect personal health information contained in designated health information banks (HIBs) of the Ministry of Health or health authorities. The Provincial Laboratory Information Solution, the Client Registry/Enterprise Master Patient Index and the Provider Registry are examples of HIBs. The E-Health Act includes the following provisions:

- allows individuals to issue disclosure directives to block access to (or "mask") some or all of their personal health information stored in HIBs
- prohibits disclosure of personal health information from a HIB for market research purposes
- establishes a Data Stewardship Committee (DSC) made up of representatives of health authorities, health professions including Doctors of BC and the College of Physicians and Surgeons and the public to evaluate data access requests for research purposes
- permits patient contact information to be disclosed for the purposes of recruiting individuals to participate in health research, but only with the prior approval of the Information and Privacy Commissioner
- adds new whistle-blower protection to protect individuals who report privacy breaches to the chief data steward or the Information and Privacy Commissioner and to encourage good faith reporting to enhance privacy protections
- establishes penalties for privacy and security breaches in the HIB (the penalty for a privacy breach in HIBs is a "fine of up to $200,000")

There is a patchwork of other health laws that apply to specific types of personal health information. The following Acts may apply depending on the context: Continuing Care Act (s. 5)

- *Continuing Care Act* (s. 5)
- *Health Act* (ss. 9 and 10)
- *Hospital Insurance Act* (s. 7)
- *Pharmaceutical Services Act* and the Information Management Regulation
- *Public Health Act*
- Health Act Communicable Disease Regulation

Role of the Information and Privacy Commissioner for BC

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

If patients or employees have concerns related to privacy and security of their personal information, they can contact the Office of the Information and Privacy Commissioner (OIPC) for British Columbia at info@oipc.bc.ca. Also, if patients or employees are dissatisfied with how their privacy complaint was addressed by the practice or the College of Physicians and Surgeons, they can file their complaint with the OIPC.

More information on privacy and access to information rights in British Columbia, the role of the Information and Privacy Commissioner and privacy legislation in BC can be found at www.oipc.bc.ca.

EMRs vs EHRs: What is the Difference?

An EMR generally refers to an electronic version of the traditional paper-based medical record used within a private practice setting. The collection, use and disclosure of personal health information in an EMR is governed by PIPA. The EMR is a comprehensive record of health information compiled in the context of a direct patient-provider relationship and is under the custody and control of the physician providing primary care.

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.

Canada Health Infoway defines an EHR 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. An EMR can be a potential 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. An EHR may also have a patient portal whereby patients can access their own records on-line.

EMRs and EHRs both offer considerable opportunities for improving patient care, safety, and health outcomes, including ways to improve efficiencies and cost-savings in the provision of care. While numerous benefits are evident in EMRs and EHRs, they present similar challenges in terms of meeting the expectations of patients and protecting personal health information

A province-wide EHR has not yet been fully implemented, but there are a number of provincial repositories for personal health information already in place. These include PharmaNet, the Provincial Lab Information System, the Panorama public health information system as well as the Client and Provider Registries. Various EHRs have been implemented in health authorities. The governance of those EHRs rests with the health authorities governed under FIPPA.

Collaborative Care and EHRs

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 clinics within health authorities. With such new forms of practice and with institutional or provincial EHRs, the sharing of personal health 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, personal health 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 personal health information by persons or organizations beyond the circle of care.

With varying amounts 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 PIPA and FIPPA is complex, and it is important that information-sharing meets the requirements of both pieces of legislation. Tools such as obtaining consent, role--based access, opt out, masking, and audits can be

used to protect patient privacy while sharing information appropriately and efficiently to support the delivery of care.

Ten Essential Steps for PIPA Compliance

This section will identify 10 essential steps that physicians in private practice need to take in order to comply with PIPA.

The following 10 steps summarize the key responsibilities that physicians have under PIPA:

- Step 1 – Be Accountable
- Step 2 – Identify Purpose
- Step 3 – Obtain Consent
- Step 4 – Limit Collection
- Step 5 – Limit Use, Disclosure, Storage and Retention
- Step 6 – Maintain Accuracy
- Step 7 – Employ Safeguards
- Step 8 – Be Transparent
- Step 9 – Provide Access
- Step 10 – Permit Recourse

Step 1 – Be Accountable

Accountability in relation to privacy is the acceptance of responsibility to protect personal information. In order to demonstrate accountability and compliance with the *Personal Information Protection Act* (PIPA), organizations should have a comprehensive privacy management program.

The person responsible for structuring and managing a privacy management program is the organization's privacy officer. In a physician's practice, it is recommended that the physician act as the privacy officer. In a solo practice, the physician is the de facto privacy officer, while in a clinic or group practice, one physician should be designated as the privacy officer. The privacy officer is answerable to the College of Physicians and Surgeons and the Office of the Information and Privacy Commissioner.

The privacy officer must do the following to establish and maintain a privacy management program for the practice:

- Compile a personal information inventory that documents the types of personal information that the practice collects and how and where it is stored.

- Develop internal privacy policies and procedures in relation to the obligations of the practice under PIPA and monitor compliance with them.
- Ensure all service contracts and information-sharing agreements include adequate privacy protective provisions.
- Put systems in place for responding to access requests, requests for correction, and complaints from patients.
- Institute mandatory privacy training and education for physicians and staff.
- Use risk assessment tools to identify and mitigate privacy impacts of new initiatives or services that involve the collection, use or disclosure of personal health information.

This Toolkit includes guidelines that are a useful starting point in demonstrating accountability by formulating privacy policies and procedures in areas that present particular challenges from a privacy perspective. These topics include the following:

- Patient consent for collection and requirements to notify patients
- Administrative and physical security controls to protect medical records
- Technological security controls and role-based access for EMRs
- Using email or fax
- Photography, videotaping and other imaging
- Responding to a privacy breach
- Using and disclosing personal health information for secondary purposes such as research
- Protecting medical records outside the practice
- Protecting medical records when leaving the practice
- Retention and secure destruction of medical records
- Informing patients about the privacy management program and their information rights

Privacy officers may also wish to develop policies and procedures on other topics depending on the practice and the nature and volume of the personal information in its custody or control.

All components of a privacy management program should be reviewed and assessed by the privacy officer on a regular basis and revised as necessary. For example, the practice may need additional security controls or improvements to privacy training and education for employees.

For further information regarding a privacy management program and the responsibilities of a privacy officer, a guidance document entitled Getting Accountability Right with a Privacy Management Program is available on the website of the Office of the Information and Privacy Commissioner.

Step 2 – Identify Purpose

PIPA provides individuals with the right to know what personal information is being collected, used or disclosed by the practice, and for what purposes. PIPA also requires that personal information only be collected for purposes that a reasonable person would consider appropriate in the circumstances. If it is not possible to identify the purpose for the collection, or if the purpose would not be appropriate to a reasonable person, the practice should not collect the personal information. Each practice should assess its information management practices to define and document the purposes for which personal health information is collected, used and disclosed.

Step 3 – Obtain Consent

Under PIPA, consent for the collection, use, and disclosure of personal information for direct health care purposes in BC operates primarily on an "implied consent" model. Implied consent usually extends to parties who provide care to a patient and form part of a patient's "circle of care" (e.g., specialists, referring physicians, lab technologists).

There are two types of implied consent: "deemed" consent or "opt-out" consent. Deemed consent may be relied upon if the information was voluntarily provided by the patient for purposes that are obvious to a reasonable person (e.g., for the purposes of ongoing care and treatment by the physician). Opt-out consent requires the physician to provide the patient with notice regarding the purpose for the collection, use or disclosure and provide the patient with a reasonable amount of time to decline (e.g., notification that the patient's personal information will be disclosed to a public body for the practice's billing purposes). Consent must always be voluntary and informed.

Express consent from a patient is required when personal information is intended to be collected, used, or disclosed outside of the circle of care by individuals who do not have implied consent or for secondary purposes such as research (see Guidelines for Secondary Use of Personal Health Information for Research). Express consent is signified by the individual willingly agreeing to the collection, use, and disclosure of personal information for a defined purpose (also known as the "opt-in" model). Express consent can be given verbally or in writing, but consent in writing may provide stronger evidence that it was given if consent is later challenged. The individual has the right to expressly withhold or withdraw consent at any time without retribution.

Step 4 – Limit Collection

A practice should collect only the minimum amount of personal information that is necessary to achieve the purpose for the collection.

Step 5 – Limit Use, Disclosure, Storage and Retention

A practice must use and disclose personal information in accordance with the purposes for collection. Consent is required for use and disclosure of personal information for new purposes, unless it is otherwise authorized by PIPA. Information should be kept only for as long as necessary to meet the original purposes or as required by the bylaws of the College of Physicians and Surgeons. The bylaws currently require that medical records be retained for at least 16 years from the date of last entry or from the age of majority. Records containing personal information (whether paper or electronic) should be disposed of appropriately, safely, and definitively when they are no longer required. For more information, see Guidelines for Secure Destruction of Personal Health Information and Guidelines for Protecting Medical Records When Leaving a Practice.

If the personal information of British Columbians is stored or accessed outside of Canada, there is a risk that other jurisdictions will not offer the same (or any) legal privacy protections for that data. While PIPA does not prohibit storage and access to personal information from outside Canada, it is recommended that physicians avoid storing personal information outside of Canada and prohibit access to such records from outside Canada without express patient consent. This includes using cloud-based software where data may be stored outside Canada.

Step 6 – Maintain Accuracy

Physicians must ensure that medical records are up-to-date and accurate. The privacy officer should develop procedures that will ensure information is collected and maintained accurately. For example,

- Forms can be designed and used to ensure all necessary personal information is collected.
- Questions can be asked on each patient visit to verify certain personal information.

Under PIPA, individuals have the right to request that their personal health information be corrected if they believe it is not accurate or complete. This right applies to correcting factual errors or omissions in the personal information of the requesting individual, and does not apply to opinions or the personal information of third parties. Individuals (or their legally authorized representative) may make a request for

correction in writing (See Form – Patient's Request to Correct Personal Information) and a practice must respond within 30 working days of receiving a request.

In order to make the correction, the practice must be satisfied on reasonable grounds that the correction should be made. If a correction is made, a copy of the amendment must be sent to each organization to which the inaccurate or incomplete information was disclosed within the past year. If no correction is made, the practice is required to annotate the information with the correction that was requested but denied, and reasons for not making the correction must be provided to the requesting individual. Requests for corrections to professional reports or expert opinions are usually annotated.

The 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 or take the matter to the Office of the Information and Privacy Commissioner (OIPC). For more information, see Guidelines for Ensuring Accuracy of Medical Records and Responding to Patient Correction Requests.

Step 7 – Employ Safeguards

A practice must implement reasonable security safeguards to protect personal information against loss, theft or other unauthorized access, use or disclosure. Safeguards refer to administrative, physical and technical measures, and may include a combination of policies, practices and software that protect personal information. The sensitivity of the personal information informs what types of safeguards are appropriate in the circumstances, irrespective of the form in which a medical record is stored (paper, electronic, digital, or otherwise). For more information, see Guidelines for Protecting Medical Records Outside the Practice.

Medical 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 in which the information is stored.

The following are best practices in safeguarding medical records and other personal information stored by the practice. Note that a combination of measures may be required during the transition from paper-based medical records to EMRs where both methods of record-keeping may be used in parallel.

In order to protect medical records, it is recommended that staff:

- wear building passes/photo ID if issued
- verify that persons who don't look familiar have a legitimate reason to be there

- know how to respond if suspicious behaviors are noticed
- not disclose confidential information about how the practice's security systems operate
- sign confidentiality agreements that specify obligations and expectations including consequences for inappropriately collecting, using or disclosing personal information

Paper records should be:

- retrieved promptly from fax machines or photocopiers
- clearly labelled
- placed in a location that prevents members of the public from viewing the records (e.g., avoid leaving medical records at the reception desk where other patients can see them)
- returned to the filing location as soon as possible after use
- stored:
    - on-site wherever possible
    - securely within the practice (e.g., in locked cabinets)
    - in a location where members of the public cannot access the contents (e.g., in a locked, separate room)
- tracked if being transferred by confirming that the records have arrived at their specified destination
- kept secure at all times if taken off-site

In order to protect personal information stored in EMRs, staff should:

- when using any system or application, log out of computer systems or applications when not in use or unattended
- keep workstations positioned away from public view and access
- memorize or use a secure password manager instead of writing down passwords
- not share an assigned user ID and password with others

The privacy officer should also do the following to protect personal information stored in EMRs:

- Create a unique user ID and strong password for every authorized user.
- Grant role-based access to staff working in the practice on an individual basis based on a "need to know" and "least privilege" principles.
- Revoke user IDs and passwords as soon as authorized users resign or are dismissed.
- Install strong, up-to-date, industry-standard encryption.
- Implement password changes forced at regular intervals.
- Install firewall software and regularly update internet-based computer systems.

- Create audit trails to track when a patient record is accessed and by whom, including date and time.
- Verify that data backup methods and disaster recovery plans are in place and are periodically reviewed and tested.
- Activate password protected screensavers or auto log out for computers after a period of inactivity to avoid unauthorized viewing.
- Consider installing a privacy screen filter to prevent viewing of the screen from an angle.

For more information, see Guidelines for Electronic Medical Records and Role-Based Access.

Step 8 – Be Transparent

A practice should be transparent about its information management policies and procedures, and provide this information to individuals upon request. This includes providing information to patients and employees about what personal information the practice collects on the basis of consent, the purposes for which the information is used, to whom it is disclosed, how it is protected, and how an individual may access or correct their own personal information. This can be achieved through patient handouts or posted notices. See these samples:

- Patient Handout – Privacy of Your Personal Health Information
- Privacy Policy Template

Step 9 – Provide Access

Patients and employees are entitled to access their personal information in the custody or control of the practice. A practice may charge a minimal fee for such access, unless the information is that person's employee personal information. For more information, see Guidelines for Responding to Patient Requests to Access Their Personal Health Information and Form – Patient Request for Access to Personal Information.

The privacy officer should develop procedures that allow a person to have access to their own records. The process should allow both patients and employees to access and request correction of their personal information.

These procedures should set out what minimal fees will be charged for patient access to records. No fee can be charged for providing access to a person's employee personal information. The minimal fee is intended to recover some of the actual and necessary costs incurred by the practice to provide access, and may include the costs associated with locating, retrieving, producing and copying a record, preparing

the record for disclosure and postage or shipping costs. The fee must not generate any profit, and does not usually include reviewing the records to make sure the practice is complying with its obligation to withhold certain types of information.

Information that should be withheld includes:

- personal information of other individuals
- information that could reasonably be expected to threaten the safety, physical or mental health of a third party
- information that could cause immediate or grave harm to the individual who made the request
- information that is subject to solicitor client privilege

When charging fees, the practice must provide the applicant with a written estimate of the total fee, and may require the applicant to pay a deposit before processing the request.

Step 10 – Permit Recourse

Individuals, including patients and employees, have the right to challenge a practice's compliance with PIPA. PIPA requires a practice to develop a process to respond to such complaints. If the individual who made the complaint is not satisfied with the practice's response, he or she has the right to make a complaint to the College of Physicians and Surgeons at www.cpsbc.ca, and to the Office of the Information and Privacy Commissioner at www.oipc.bc.ca. Resolving complaints through the practice's privacy officer can be a more efficient way to address patient or employee concerns relating to privacy and access to information issues. For more information, see Guidelines for Responding to Patient and Employee Complaints and Guidelines for Responding to Patient Requests to Access Their Personal Health Information.

Guidelines for Confidentiality Agreements, Service Contracts and Information Sharing Agreements

This section will:

- identify key elements to include in confidentiality agreements
- identify key privacy-protective elements to include in service contracts
- identify key elements to include in information sharing agreements (ISAs)

Service providers, suppliers, partners, employees, and others may be engaged by physicians to assist them in their practices. During their work, these third party individuals or organizations are likely to be

exposed to personal information in the custody and control of the practice. Therefore, depending on the situation, privacy-protective contractual clauses, confidentiality agreements, and ISAs should be in place to ensure that third parties comply with the practice's expectations that personal information will be appropriately safeguarded in compliance with PIPA. If third parties must collect, use or disclose personal information as part of their contractual obligations, it's important to ensure they have the legal authority to do so.

Confidentiality Agreements

A physician's obligation to safeguard personal information means having internal staff and third parties who have access to personal information sign a confidentiality agreement. Some of the elements to be included in a confidentiality agreement include establishing what personal information must be kept confidential and what security safeguards are required, clarifying who has custody and control of the personal information, and what the consequences are for non-compliance with the agreement. These sample confidentiality agreements may be used as a guide:

- Confidentiality Agreement for Employees
- Confidentiality Agreement for Third Parties
- Confidentiality Agreement for Health Authority Employees Working in a Physicians Private Practice

Privacy Considerations in Service Contracts

Before entering into a service contract with an external service provider (e.g., application service provider, EMR vendor, record destruction services, storage retrieval services), physicians can protect personal information by ensuring:

- Service providers have effective and comprehensive information management practices that are at least equal to those implemented by the practice
- Contracts include the appropriate security arrangements and privacy protection clauses

These requirements should be monitored and enforced by the service provider. For service providers that frequently handle sensitive personal information as part of the contract, the practice should undertake audits to verify compliance.

When preparing a contract with a service provider, the following elements may be included:

- Identification of:

- all applicable privacy laws and clearly state that the service provider must comply with these as well as their own privacy laws and policies
- the purposes for which the personal information can be collected, used, or disclosed based on the patient's initial consent and restrictions on any further use to those purposes, except as permitted or required by law
- who will maintain custody or control of the personal information
- all reasonable physical, administrative and technical safeguards to protect the personal information from unauthorized access, collection, use, disclosure, copying, modification or disposal, or similar risks
- any financial or other consequences that may result from non-compliance with the contract

- A requirement that service providers:
  - only collect, use, access and retain the information provided to them as identified in the contract
  - only allow access to subcontractors after the practice is made aware of it and has approved their access
  - allow the practice to access its information upon request and never deny access because of a disputed payment for services
  - notify the practice if any personal information has been lost, stolen, used, or accessed in an unauthorized manner
  - report any privacy breach or security incident within an agreed-upon timeframe
  - return or destroy personal information when the contract ends as specified
- It is recommended that only service providers who store and access personal information 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. In these circumstances, the contract should specify:
  - where personal information is being stored, who has access, and what security provisions are in place
  - in situations where there are remote access capabilities, from what locations personal information may be accessed
  - for any aspect of the service provider's operations that are out-of-country, the contract binds the service provider to PIPA, as their own jurisdiction may not have any or adequate privacy laws, compared to BC standards

For information on service contracts for record storage and destruction, see:

- Guidelines for Protecting Medical Records When Leaving a Practice

- Guidelines for Secure Destruction of Personal Information

Guidelines for ISAs

If sensitive personal health information is shared with third parties on a frequent and regular basis (e.g., with health authorities or specialists), an information-sharing agreement (ISA) should be in place. ISAs help clarify how personal health information will be exchanged and how it will be protected.

ISAs can also assist in supporting new and evolving models for structuring a practice. For example, physicians may implement different organizational models based on whether they choose to have electronic medical records (EMRs) or a paper-based system. If personal health information in an EMR is shared with third party care providers, ISAs can help determine who is accountable for the personal information affected, who has custody and control, what the authorities are for collecting, using and disclosing personal information, and what security safeguards are in place to protect personal information.

An ISA will usually:

- reference all applicable legislation that provides the legal authority for collection, use, and disclosure of personal information
- identify:
    - types of information each party will share with each other
    - the purpose for data sharing
    - permitted uses for the specified purpose
    - disclosure restrictions
    - retention periods
    - who has custody and control of the information
- describe:
    - what personal information will be shared
    - who will have access and under what conditions
    - how personal information will be exchanged
    - security safeguards in place to protect personal information
    - secure destruction methods when retention expires
    - processes for:

- responding to access requests by individuals whom the personal information is about
- ensuring accuracy
- managing privacy breaches, complaints, and incidents
- terminating the agreement

The Canadian Medical Protective Association (CMPA), in partnership with the Canadian Medical Association, has produced Data Sharing Principles for EMR/EHR Agreements.

Guidelines for Consent and Masking Options

This section will:

- define physician responsibilities regarding a patient's implied, deemed and express consent for the collection, use, and disclosure of their personal information
- discuss masking options and physician responsibilities in EMRs and EHRs when personal information is masked by way of disclosure directive or protective words

Implied and Express Consent

Under PIPA, the collection, use, and disclosure of personal information by a practice operate primarily on an "implied consent" model. Individuals who form part of a patient's "circle of care" (e.g., specialists, referring physicians, lab technologists) may collect, use, disclose and retain personal health information for the purposes of ongoing care and treatment on the basis of "implied consent".

"Implied consent" must be voluntary and informed, and physicians have a responsibility to provide adequate information to patients on how the practice manages personal health information (See Ten Essential Steps for PIPA Compliance and the handout Patient Handout - Privacy of Your Personal Health Information). "Implied consent" may be established when an individual is provided with a notice about the collection, use, and disclosure of personal health information in a form they can reasonably understand and for reasonable purposes given the sensitivity of the personal health information. Also known as the "opt-out" model, "implied consent" is established after the individual is provided with a reasonable opportunity to decline. 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.

Another form of consent that may apply to a patient's circle of care is "deemed consent". "Deemed consent" applies only in situations where the purpose of the collection, use or disclosure of personal

information at the time consent is sought is clear and obvious to a reasonable person. The individual must also voluntarily provide their information for that specific purpose.

"Express consent", also known as the "opt-in" model, is a person's verbal or written agreement to the collection, use and disclosure of their personal information for a defined purpose. Express consent from a patient is required when personal information is intended to be collected, used, or disclosed outside of the "circle of care" or for secondary purposes, such as education or research. For more information, see Guidelines for Secondary Use of Personal Health Information for Research. If the practice anticipates using personal health information for educational or research purposes, these purposes should be clearly stated in the practice's privacy policy and in the patient Consent for Research form.

Masking Options (Disclosure Directives and Protective Words)

Patients may have the option to restrict access to certain personal health information about them that is stored in EHR and EMR systems. This privacy protective feature of an EHR or EMR system is known as "masking", and patients should be informed of this right. The following are examples of "masking" options in EHR systems in BC.

The **Provincial Lab Information Solution** (PLIS) is a provincial repository of lab information that has been designated as a health information bank under the **E-Health Act** (Personal Health Information Access and Protection of Privacy Act). A person whose personal health information is contained in this repository may make a disclosure directive that restricts access to their lab results for clinical purposes. Once a disclosure directive is made through the addition of a "keyword" to the record, lab results can only be accessed by an authorized user for clinical purposes, after the person who made the disclosure directive shares their "keyword" or if there is a need to provide urgent or emergency health care.

Under the **Pharmaceutical Services Act**, a person may request that a "protective word" be attached to their medical and claims history recorded in **PharmaNet**. They may also request that a "protective word" be applied to the record of a minor or adult for whom they have authority to make such decisions. Similar to the disclosure directive model, once the "protective word" is attached, authorized users of PharmaNet can only access medication information for clinical purposes after the person shares their "protective word". Some authorized users may also request the protective word be removed to allow them to provide care in an emergency where neither the person nor their representative is able to provide the "protective word". For more information on PharmaNet protective words, see Protective Word for a PharmaNet Record.

Some health authorities permit patients to mask personal information in their EHR systems. For example, patients can make a disclosure directive in the **CareConnect** system at **Vancouver Coastal Health Authority**.

Many EMR applications have explored and implemented "masking" options. The ability to mask 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 some or all of their personal information.

Physicians should inform patients about the option to mask personal information in their record, as well as the effects of "masking" on delivery of care. If a competent patient decides to mask their record, physicians must:

- honour the patient's decision and only access the personal information with express consent
- 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

Alternatively, in the absence of an emergency, if the lack of masked information creates a situation where the physician feels the patient's safety is at risk, the physician can refuse to provide treatment. The physician should explain the reasons for their decision not to treat the patient and note all relevant discussions in the patient's medical record.

A physician who is treating a patient whose information has been masked and who does not give the physician express consent to permit access, still has an obligation to obtain a proper history from the patient. Taking a proper history may elicit relevant information, even if that information is masked. To the extent that a patient refuses to discuss relevant information, this refusal should also be adequately documented.

Guidelines for Electronic Medical Records and Role-Based Access

This section will:

- Summarize privacy and security considerations during the transition from paper to EMR.
- Define role-based access and identify key considerations related to EMR implementation.
- Identify privacy and security best practices.

Making the Transition to EMR

The 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 transition from a traditional paper-based patient record to an electronic system that uses new technologies 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.

During the transition to EMR, the following recommended steps may be of assistance:

- Understand existing paper-based workflow processes including data flows and modify processes as necessary to integrate the use of EMR to achieve the greatest benefits.
- Assess existing privacy and security policies and practices and revise them to reflect the use of EMR and personal information in electronic format.
- Update staff privacy training to incorporate an understanding of the changes associated with EMR.
- Begin by scanning paper records into electronic format or start entering data into the EMR beginning on day one.
- Retain one original medical record and once the information has been fully transitioned to EMR, the original paper record may be securely disposed of.
- If only part of the paper record is transitioned to EMR, retain the remainder of the paper record as part of the original medical record.
- Save scanned copies of paper records in "read-only" format.
- If using optical character recognition (OCR) technology to convert records into searchable and editable files, retain either the original record or a scanned copy.
- Ensure patients still have access to their complete information upon request, even if the information now exists in a combination of formats (paper, electronic, digital).

Role-Based Access

Role-based access control is an essential functionality in an EMR system. Role-based access uses information technology to protect the personal information of the patient by ensuring that access to the patient's personal information is based on the "need to know" and **"**least privilege**"** principles.

The role-based access model identifies all possible roles that require access to a patient's personal information, and assigns each of these roles access to only the type and amount of personal health information needed to perform the job function. For example, specific permissions (e.g., reading, writing, printing) can be assigned to certain personal health information (e.g., lab results, medication information, registration information) based on the job duties of the person who has access.

Roles must be defined for all of the various users, whether they are employees or otherwise, who access the EMR. These include clerical staff, billing services, nurses, students, residents, physicians-in-training, locum physicians, on-call group, visiting specialists, and other physicians within the practice. When assigning a role, a prudent physician will always assess the degree to which access to the patient's personal information is truly necessary for that person to perform their duties.

Implementing this model also allows for ease of account management when setting up new users and modifying accounts. Role-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 practice. It must also allow for exceptions to the standard role and permissions, provided it is authorized and necessary for the performance of job duties.

An authorized role alone does not entitle an individual to access a given record, as the individual must have a "need to know" based on that individual's provision of care to the patient. "Need to know" can frequently become "want to know", which may not meet the required threshold for granting authorized access or may lead to workplace snooping.

When determining which functional areas and permissions should be assigned to each role and user, ask:

- Can existing users currently access all of this information?
- Does each of these roles truly need access to all areas of available information?
- Are the users unable to carry out the requirements of their job if they do not have access to this information?
- Can the patient suffer harm if the user does not have access to this information?
- Are there professional practice standards requiring the user to have access to this information?
- Is the information required to support the care of the patient across the continuum of care?
- Does the user require 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?

When defining roles, assigning access and granting permissions associated with each role, ask:

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

Privacy and Security Considerations

Physicians are responsible for data stewardship, and assume responsibility for any access to personal health information, including by staff, contractors and delegates.

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

- automatic log off feature
- strong, up-to-date, industry-standard encryption applied to EMR data and portable electronic devices
- audit trails to record user access
- allowance for correction/annotation of information
- ability to mask/unmask sensitive data (See Guidelines for Consent and Masking Options)
- unique user IDs and passwords
- 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 practice privacy and confidentiality policies
- ensuring that audit log capability is activated in the EMR system to track all user access to patient information for the purposes of compliance monitoring and incident investigation
- managing user accounts including adding, modifying, and de-activating user accounts on a regular and timely basis
- confidentiality disclaimers on printed reports
- robust backup and recovery procedures

Guidelines for Ensuring Accuracy of Medical Records and Responding to Patient Correction Requests

This section will:

- identify requirements to keep paper and electronic records accurate
- explain patients' rights to verify the accuracy of their medical records and ask for corrections

Regardless of the method used to record personal information, the designated privacy officer must ensure that the information is up-to-date and accurate. Personal health 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 can range from personal embarrassment to physical harm or even death.

Under PIPA, individuals have the right to request corrections to their personal information if they believe it is not accurate or complete. Of course, professional or expert opinions cannot be corrected or changed. If the correction is reasonable, the privacy officer must amend the information as requested, and send a copy of the amendment to each organization that received the inaccurate or incomplete information within the past year. If no correction is made, the privacy officer must explain the reasons for refusing the correction, and annotate the personal information with the correction that was requested but not made.

A practice's privacy policy should describe how personal health information is kept accurate and how patients may request corrections to their information. Patients (or their legally authorized representative) may make a request for correction in writing (see Form – Patient's Request to Correct Personal Information) and a practice must respond **within 30 working days** of receiving a request.

The 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 or make a complaint to the OIPC.

Best practices for maintaining accuracy include that personal health information in paper-based medical records should be:

- written clearly, legibly, and in such a manner that it cannot be erased
- readable on any photocopies or faxes
- accurately dated, timed, and signed, with the name of the author printed alongside the first entry
- wherever possible, written with the involvement of the patient

- clear, unambiguous, and written in terms that the patient can understand (abbreviations, if used, should follow common conventions)
- for any alterations or additions, dated, timed, and signed in such a way that the original entry can still be read clearly
- when not making a requested correction, noted clearly with details of the request and reasons for not making changes
- organized in a consecutive or chronological order

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

EMRs should:

- have the ability to correct information through an amendment (e.g., the original data must not be modified or deleted as history should be maintained)
- accurately date and time-stamp a correction, recording who made the amendment
- allow for an annotation whenever a correction is requested but not made
- be able to generate a copy of a medical record with the amended information and correction history

Guidelines for Photography, Videotaping, and Other Imaging

This section will:

- describe reasonable practices for protecting personal information when using photography, videotape, digital imaging, or other visual recordings
- identify what needs to be done before, during, and after photographing or recordings patients

These guidelines should be followed when using photography, videotape, digital imaging, or other visual recordings, for the purpose of providing care to that patient, for education, or for research.

If photographs or videotape recordings that identify patients are required for medical, surgical or any other procedures for the purpose of providing care, the practice should obtain express written consent from the patient. This consent does not authorize the collection, use or disclosure of the images for any other purposes such as education, scientific publication or research unless these purposes are expressly stated in the consent form.

Before photographing or recording patients, physicians are required to:

- Obtain express consent:

- from patients to the collection, use and disclosure of photographs or recordings
  Although verbal consent is sufficient, best practices include that the patient is provided with a written consent form that provides relevant information (including the purposes for collection, use and disclosure) in a way that the patient can understand (translations should be provided where necessary prior to signing the form), and the patient is given a reasonable amount of time to consider the information.
- from a parent or guardian if the patient is a child who is incapable of exercising their legal rights
- from a personal representative if a patient is deemed incapable or incompetent
- for any use or disclosure beyond the original purpose

- Ensure the patient understands the:
  - purpose for which the photograph or recording is taken and how it will be used
  - who will be allowed access to it
  - whether copies will be made
  - how long the photograph or recording will be kept
- Inform the patient that:
  - refusal to consent will not affect the quality of care being offered
  - their consent can be withdrawn at any time without consequence
- Immediately stop the photography or recording session if the patient withdraws consent

After the photography or recording session, best practices dictate that physicians are responsible for:

- asking the patient whether they wish to withdraw consent to the use of the photograph or recording
- if the patient withdraws consent, ensuring the photograph or recording is securely destroyed or erased as soon as possible
- ensuring all photographs, videotapes, recordings or images are identified with the patient's name, identification number, and date or a numeric identifier
- filing photographs with the patient's medical record
- storing videotapes or recordings with the patient's medical record or if stored separately in a secure area, noting the location of the photos, recordings, or images in the patient's medical record
- ensuring the same level of security over photographs, videotapes, recordings or images as for all confidential medical records

Where photographs, videotapes, recordings, or images may be shown to third parties other than the immediate health care team responsible for the patient's care, express consent may be necessary. The patient should be:

- made aware of and understand that the photographs or recordings may be shown to people who may not have any responsibility for their health care
- 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

If the patient cannot be identified in the photograph or recording, it is sufficient for the physician to provide the patient with an oral explanation regarding the purpose of the proposed recording and note this information in the patient's chart. No photograph or recording should be made contrary to the patient's wishes.

In exceptional circumstances, the photograph or recording may be captured without the patient's consent. For example, if the patient's consent for capturing a photograph or recording cannot be obtained in a timely way or the patient is unable to give consent (e.g., due to the patient being under anaesthesia), and the collection of this personal information is clearly in the interest of the individual or is necessary for the patient's medical treatment. The physician must subsequently request the patient's consent prior to using or disclosing the photograph or recording.

Guidelines for Protecting Medical Records When Leaving a Practice

This section will:

- describe best practices regarding medical records when leaving a practice
- identify key considerations and elements of contracts with a service provider to provide storage, retrieval, or destruction of medical records

When a medical practice is closed, replaced, or relocated outside of BC, physicians have a professional and legal duty to use reasonable efforts to do the following with medical records:

- Arrange secure transfer to another physician who agrees to accept responsibility for the patient.
- Arrange for secure storage and retrieval for the remaining retention periods.
- Securely dispose of medical records where the retention period has expired.

Custodians must understand where medical records are being stored, who has access to them, what security provisions are in place and from what locations they may be accessed (e.g., if there is remote access for support). Additional guidelines related to ensuring continuity of care for patients who require it

and the preservation of medical records are available on the College of Physicians and Surgeons website under Standards and Guidelines: Leaving Practice.

Best practices for protecting medical records when leaving a practice include ensuring:

- patient notification includes information on the:
  - departure date
  - how patients can obtain a copy of their records or request transfer of a copy of them to a new physician
  - how patients may access their records if they are to be stored by a service provider
  - reasonable fee that may be charged for providing this service
- patient authorization is obtained
- transfer of medical records occurs in accordance with section 3-7 of the College Bylaws
- the original record is retained under college retention guidelines for the purposes of future complaints or legal action (medical records must be retained for at least sixteen years from the date of last entry or, in the case of minors, sixteen 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)
- all medical record documentation is accurate and completed before they are archived
- there is a process in place to support any outstanding patient work that may be in progress (e.g., pending lab tests that may require follow-up)
- if the records are no longer required, secure records disposition procedures are followed (see Guidelines for Secure Destruction of Personal Information)

If a service provider is engaged to provide storage and retrieval services for medical records for the remaining retention period, ensure this is done under a service contract that places the following kinds of obligations on the service provider:

- Maintain the confidentiality of all medical records stored, providing access to information only to authorized representatives of the physician or with written authorization from a patient or legal representative.
- Upon request of the physician, promptly return all confidential medical records without retaining copies.
- Prohibit the use of medical records for any purpose other than what was mutually agreed upon (this includes selling, sharing, discussing or transferring any medical records to unauthorized business entities, organizations, or individuals).

- Use reasonable administrative, physical and technical safeguards to protect against theft, loss, damage, and unauthorized access of medical records.
- When specified by the physician, securely destroy medical records at the end of the retention period (see Guidelines for Confidentiality Agreements Service Contracts and Information Sharing Agreements).

While PIPA does not prohibit storage and access to personal information from outside Canada, it is recommended that physicians avoid disclosing personal information outside of Canada without express patient consent. If any aspect of a service provider's operations occurs out-of-country, it is recommended that the physician ensure the legal agreement binds the service provider to comply with BC's privacy laws, in order to avoid situations where the service provider's jurisdictions does not have privacy laws or such laws are not adequate by BC standards.

Guidelines for Protecting Medical Records Outside the Practice

This section will identify best practices for protecting medical records outside of the practice.

Physicians have a legal and ethical obligation to respect patient confidentiality and to protect personal health information. The CMA Code of Ethics requires physicians to protect the personal health information of their patients. PIPA requires that physicians take reasonable measures to protect patients' personal information from risks of unauthorized access, use, disclosure and disposal and sets out consequences for violation. The Information and Privacy Commissioner has 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 Medical Records Outside the Practice

There are times when physicians and their staff may need to access personal information remotely while travelling, at home or in another location. This includes transporting records by car or airplane, working from home, attending meetings or conferences or making visits to a patient'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. With EMRs and other forms of electronic communication, physicians and their staff are also able to connect to their practice network and may have access to sensitive personal health information from anywhere in the world.

Physicians must implement reasonable safeguards, including administrative, physical and technical measures, to reduce the privacy risks of accessing personal health information outside the practice.

Conversations

When having conversations outside the practice:

- Avoid discussing a patient's personal health information in public areas such as on elevators, in stairwells, while travelling by public transit or airplanes, in restaurants or on the street.
- Avoid using cell phones to discuss a patient's personal health information while in transit as these conversations can be intercepted or overheard.
- Use a dedicated phone line with password protected voicemail when working from home.

Paper Medical Records

When using paper medical records:

- only remove medical records from the practice when it is absolutely necessary for performing job duties
- require all staff to obtain approval from their supervisor before removing medical records from the practice
- use a sign-out sheet to document who is removing a medical record, the name of the individual whose personal information is being removed, and the date the record is being removed
- leave the originals in the practice, if possible
- take only the minimum amount of personal information required to perform the task
- if the records are large, consider using a courier to transport them to their destination
- place records in confidential folders, transport them in a secure container, and keep them under control at all times, including meal and break times
- keep records locked in a desk drawer or filing cabinet when working from home to reduce unauthorized viewing and access by family members or friends
- if transporting medical records by car, keep them locked in the trunk before the start of the trip
- never:
    - leave medical records unattended, even if they are stored in the trunk as these are no less accessible to thieves than the front seats
    - examine medical records in public places where they may be viewed or accessed by unauthorized individuals (e.g., on public transit)
    - leave medical records open for view in hotel rooms (e.g., keep them in the hotel safe)

- immediately return medical records to their original storage location upon returning to the practice
- securely destroy any copies that are no longer required

Portable Devices

When accessing medical records on portable electronic devices:

- Avoid storing personal information on portable electronic devices unless absolutely necessary.
- PIPA requires that any personal information stored on a portable electronic device must be protected by industry-standard encryption.
- Wireless transfer of personal information or storage on cloud-based programs must also be protected by industry-standard encryption.
- Protect portable electronic devices containing personal information with a strong password and use a secure method, such as two-factor authentication, to grant user access.
- Keep portable electronic devices secure to prevent loss or theft (e.g., in a locked briefcase, desk drawer, container or room) and keep them under one person's control at all times, including meal and break times.
- If transporting portable electronic devices by car, lock them in the car trunk before the start of a car trip.
- Never leave portable electronic devices unattended, even if stored in the trunk.
- Remove all sensitive personal information when no longer needed 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).

Electronic Records

When accessing medical records on home computers or portable electronic devices:

- Avoid storing any personal information on the hard drive of a home computer.
- Never:
    - use public computers or wireless networks to connect to the practice network as these are not secure
    - use a laptop or home computer that is shared with other individuals, including family members and friends
    - send documents containing personal information to or from a personal or otherwise unsecured email address

- Always:
  - log off from a laptop or home computer when not in use
  - set an automatic log out to occur after a period of inactivity
  - lock home computers that are used for work-related purposes to a table or other stationary object with a security cable
  - keep home computers in a room with restricted access
  - use strong, up-to-date, industry-standard encryption and password protection for any personal information that must be stored on hard drives
  - ensure that laptops and home computers have, at a minimum, a personal firewall, anti-virus protection, and anti-spyware protection
  - ensure the latest updates and security patches are regularly installed
  - use an encrypted link to the host network, such as a virtual private network (VPN), when conducting business involving personal information over a network
  - watch out for "shoulder-surfing" where family members or friends may casually observe the screen of the laptop or desk computer

For more information, see Protecting Personal Information Away from the Office.

Guidelines for Providing Virtual Health Care

This section will:

- identify security safeguards to use when providing virtual health care
- identify patient consent requirements if systems involve access and storage of information outside Canada
- discuss implied consent in relation to disclosure to health authorities

Security Safeguards

It is essential that physicians ensure virtual health care systems have appropriate security measures and are otherwise PIPA compliant. For example, physicians should only use systems with up-to-date, industry-standard encryption for transmission of data. To reduce the amount of personal health information disclosed to companies providing virtual health care systems, physicians and health authorities should try to communicate with each other about patient medical conditions without referring to the patient's unique identifiers, where feasible.

Storage and Access Outside Canada

Certain virtual health care systems involve access to and storage of personal information outside Canada. This is permitted under PIPA but not under FIPPA, which governs health authorities. If personal information will be shared between a practice and a health authority, personal information in a health authority's custody or control must be stored and accessed only in Canada unless the health authority obtains patient consent for access or storage outside of Canada.

The physician or the health authority can obtain this consent in the following manner:

- The consent must be in writing and specify the personal information for which the individual is providing consent, the date on which the consent is effective, the purpose of the storage of or access to the personal information, and to whom it will be disclosed.
- If practicable, the consent form should also indicate the date on which the consent expires, who may store or access the personal information and the jurisdiction in which the personal information may be stored or accessed.
- Consent must be voluntary. If the patient cannot receive health care services unless they give their consent to having their information accessed or stored outside of Canada, the consent may not be voluntary. This is because health care is increasingly considered an indispensable (as opposed to optional) service. In such cases, systems that store and access personal information in Canada should be used.

Indirect Collection by Health Authorities

FIPPA requires that heath authorities only collect personal information directly from the individual (as opposed to indirectly through the physician), unless limited exceptions apply. One of the exceptions is that the individual has authorized another method of collection (e.g., by agreeing to indirect collection by the health authority). Generally, physicians have implied consent from the patient to disclose personal information to a health authority when the health authority is providing direct care to that patient. However, health authorities may not have the authority under FIPPA to collect that personal information. In situations where the physician adequately informs the patient that the patient's personal information will be disclosed to, and collected by the health authority, the health authority may collect that personal information.

Guidelines for Responding to a Privacy Breach

This section will:

- explain what constitutes a privacy breach
- identify whistle-blower protections in PIPA
- identify the four steps that physicians need to take following a suspected or confirmed breach
- explain the role of Information and Privacy Commissioner with regard to breaches

PIPA requires physicians to protect personal information that is under the practice's custody and control. Part of that responsibility involves managing privacy breaches, including taking steps to prevent them from occurring, developing a privacy breach response plan and promptly responding when a breach occurs. A privacy breach occurs when there is unauthorized collection, use, disclosure, retention, or disposal of personal information. Those activities are "unauthorized" if they occur in contravention of PIPA.

The following scenarios are common examples of how a privacy breach can occur:

- Personal information is stolen or misplaced.
- A patient's medical record or an electronic portable device containing personal health information (e.g., laptop, handheld electronic device, USB storage device) is lost or stolen.
- A letter containing a patient's diagnosis is inadvertently sent by mail, fax or electronically to an incorrect address or to the wrong person.
- A medical record is saved in a web folder that is publicly accessible online.
- A physician sells a computer previously used by the practice to a business without first deleting the personal information saved on the computer and securely wiping the hard drive.
- A physician uses their electronic access to look up the personal health information of a friend or relative who is not currently receiving treatment from that physician.

The fact that a privacy breach has occurred does not necessarily mean the practice has contravened PIPA, as certain types of privacy breaches may be unavoidable (e.g., ransomware or phishing scams carried out by sophisticated hackers). The requirement to have "reasonable" security measures does not impose a standard of perfection but requires a very high level or rigour given the sensitivity of personal health information. The practice should be objectively diligent and prudent in all circumstances and implement measures that include:

- strong, up-to-date, industry-standard encryption for electronic information
- unique passwords

- controls to restrict access
- secure data back-ups
- physical measures such as locked cabinets

For more information, see Step 7 – Employ Safeguards.

Suspected or real privacy breaches can come to a practice's attention through compliance monitoring mechanisms such as audit trails that flag unusual access, a complaint by an employee, patient, or member of the public, or through the OIPC as a result of a formal complaint.

Anyone who reports a privacy breach in good faith and on the basis of reasonable belief is protected under PIPA's whistle-blower provisions. These provisions protect an individual from being dismissed, suspended, demoted, disciplined, harassed or otherwise disadvantaged for having reported the breach, and the individual's identity may be kept confidential by the OIPC.

The OIPC has prepared guidance materials to assist in detecting, responding to, and preventing privacy breaches. The guidance materials include:

- Privacy Breach Checklist to evaluate the impact of a privacy breach and determine if notification is necessary.
- Online Privacy Breach Report Form if an organization decides to self-report a privacy breach to the OIPC.

For more information, see Privacy Breaches: Tools and Resources.

Once a privacy breach is identified, the practice must immediately respond to the breach by taking four key steps.

Step 1: Contain the Breach

Take immediate steps to contain the breach and mitigate the risk of harm by:

- contacting the designated privacy officer
- immediately containing the breach, which could involve stopping the unauthorized practice, suspending user accounts, revoking computer access codes, shutting down the system that was breached, recovering the records, or correcting weaknesses in physical security
- notifying law enforcement if the breach involves theft or criminal activity
- making sure evidence that could be used to investigate or correct the breach is not compromised

Step 2: Evaluate the Risks Associated with the Breach

As soon as possible after discovering a breach, determine the extent of the breach and potential harms that could occur as a result, by considering:

- What kinds of personal information were involved and how sensitive is that information?
- What format was the information in (paper, electronic) and how was it protected (encrypted, anonymized, password protected)?
- Was it lost, stolen or mistakenly disclosed?
- Could the personal information be misused, and if so, how?
- What was the cause of the breach?
- Was it an isolated event or is there a risk of ongoing or further exposure?
- Who and how many individuals were affected by the breach?
- What harm to the affected individual(s) could result from the breach?
- 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).
- What harm could result to the practice as a result of the breach?
- Are there risks to the public (such as health and/or safety) as a result of the breach?
- Has the information been recovered?

Step 3: Implement Notification Procedures

Consider whether the following individuals or groups need to be notified:

- individuals (whether patients or staff) whose personal information was involved in the breach
- the OIPC
- law enforcement authorities
- professional regulatory bodies (such as the College of Physicians and Surgeons)
- mutual defence organizations (such as the Canadian Medical Protective Association)
- other groups based on legal, professional, or contractual obligations

In determining whether to notify consider:

- Do any legal obligations (contractual, legislated, etc.) require notification?
- How sensitive was the personal information?
- How many people were affected by the breach?
- Was the information was fully recovered without further disclosure?
- Could the personal information be used to commit fraud or identity theft?

- Is there is a reasonable risk of physical harm, psychological harm (including humiliation or damage to reputation), or financial harm (including loss of business or employment opportunities)?
- Is there is a risk of harm to the public or to patient relations?

Individuals who are affected by a privacy breach should be **notified immediately** if it is necessary to avoid or mitigate harms that they could experience as a result of the breach. The determination of whether or not to report the breach to the OIPC should generally be made within **two days** of the breach. While PIPA does not currently include an explicit requirement for organizations to report breaches to the OIPC, doing so will assist the practice to demonstrate that it has taken reasonable steps to respond to the privacy breach and in the resolution of any complaint made to the OIPC.

The notification should include:

- the date and description of the privacy breach
- a description of the personal information that was involved in the privacy breach
- a description of potential risks of harm that could occur as a result of the breach
- steps taken to mitigate the harm
- steps planned to prevent privacy breaches in the future
- what affected individuals can do to further protect themselves and mitigate the risk of harm
- if appropriate in the circumstances, an offer for complimentary credit monitoring
- contact information for the practice's privacy officer who can answer questions
- a statement of the right to complain to, and whether or not the practice has notified, the College Of Physicians And Surgeons or the OIPC

Step 4: Prevent Future Privacy Breaches

Once immediate steps are taken to mitigate the risks, the practice, including the staff, should investigate the cause of the breach. Long-term safeguards should be developed to prevent further breaches. This may require updating privacy and security policies, performing a security audit of the practice's physical and technical safeguards, re-training employees on their privacy obligations, and undertaking a final audit to verify that the security arrangements have been implemented and function as planned. This process should generally take place **within two months** of the breach.

Guidelines for Responding to Patient and Employee Complaints

This section will:

- explain patients' and employees' rights regarding complaints related to their personal information

- identify the requirements of an effective complaint management process
- describe the ten steps of managing a complaint

Under the BC Personal Information Protection Act (PIPA), a practice must have a process to respond to complaints about its privacy practices or how personal information was handled. For example, individuals may have a complaint about the scope of records produced by the practice in response to a request for their personal information, collection practices, a disclosure of personal information without consent or a privacy breach. 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 a practice to address complaints in a timely manner, identify systemic or ongoing compliance issues and demonstrate a commitment to privacy.

In a complaint involving a privacy breach, responding in an effective and timely manner is critical. For guidance on responding to privacy breaches see Guidelines for Responding to a Privacy Breach or Privacy Breaches: Tools and Resources.

Best practices for setting up a complaint management process include the following steps:

- Decide who in the practice will be responsible for receiving, responding to and managing complaints about the practice's compliance with PIPA (this could be the designated Privacy Officer or it could be delegated to another individual).
- Develop and document a complaint procedure that is confidential, accessible, simple and easy to use.
- Develop a complaint form to assist in recording the complaint and collecting the necessary information required to investigate and respond.
- Document the process and ensure all employees are aware of the complaint management process so they can direct a 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.
- Ensure the process includes providing reasons for a decision in sufficient detail to suit the nature of the complaint.
- Reinforce that addressing a complaint quickly helps maintain or even increase the patient's trust in the practice.

Steps for Managing a Complaint

When the complaint is received in writing, record the date of the complaint and acknowledge its receipt.

- If the complaint is received verbally, record the nature of the complaint and the details.
- If necessary, contact the individual to clarify the complaint.
- Ensure that the complaint process is fair, impartial, and confidential.
- Investigate the complaint by gathering information and fully understanding the circumstances. Clarify specifics of the complaint by asking questions such as:
    - What events led to the complaint?
    - What personal information is involved and what happened to it?
    - When and where did the event(s) occur?
    - Who was involved (e.g., employees, locum physicians, visiting specialists, physicians-in-training, third party contractual employees)?
- Where a complaint is justified, determine the specific cause and
    - take measures to remedy the situation
    - communicate this to relevant employees involved
    - record all decisions and actions taken to prevent recurrence
- If a complaint cannot be substantiated, document the investigation so it can be explained to the complainant.
- Notify the complainant of the outcome and the reasons for the decision regardless of whether the complaint can be substantiated or not. Where applicable, inform him or her of the steps taken to rectify the concerns.
- Inform the complainant of the right to appeal to the Information and Privacy Commissioner, if they are not satisfied with the practice's response to the complaint, within 30 business days starting from the date the physician's office communicated to the complainant its reasons for the response.
- If applicable, prevent recurrence through techniques such as modifying or updating policies and procedures, providing employee training and implementing improved privacy and security safeguards.

Guidelines for Responding to Patient Requests to Access Their Personal Health Information

This section will:

- explain patients' rights to access their personal health information held in a practice
- identify what a physician or privacy officer should consider before responding to access requests, including timelines, exceptions to disclosure of personal information, whether to charge a minimal fee and what to do if an employee or patient makes a complaint with respect to access

Under PIPA, patients (or the patient's legally authorized representative) and employees (including volunteers) are entitled to access their personal information in the control of a practice. Practices have a legal duty to make reasonable efforts to assist an individual with their request, respond to requests as accurately and completely as reasonably possible and, where appropriate, provide the individual with the requested personal information.

Timeline

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

Exceptions

There are some exceptions where personal information may not or must not be released to a patient. For example, some of the circumstances where an organization is not required to disclose personal information to a patient include where:

- information is protected by solicitor-client privilege
- disclosure of the information would reveal confidential commercial information that if disclosed could, in the opinion of a reasonable person, harm the competitive position of the organization

An organization is required to withhold personal information in the following circumstances:

- The disclosure would reveal personal information about another individual.
- The disclosure could reasonably be expected to threaten the safety or physical or mental health of an individual other than the individual who made the request.
- The disclosure can reasonably be expected to cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request.
- The disclosure would reveal the identity of an individual who has provided personal information about another individual and the individual providing the personal information does not consent to disclosure of their identity.

PIPA allows an organization to disclose information about the mental or physical health of a patient to a health care professional for the purpose of obtaining an assessment from that health care professional about whether the disclosure of information to the patient could reasonably be expected to result in grave

and immediate harm to the patient's safety or mental or physical health. PIPA defines a "health care professional" as a medical practitioner, psychologist, registered nurse or registered psychiatric nurse. There are additional requirements for this type of disclosure, including that the practice and the health professional enter into a **confidentiality agreement** and that the information must not be used for any purposes other than making an assessment.

If the patient's access request is refused, the practice must provide the patient with reasons for the refusal.

Fees

The practice may charge a minimal fee for responding to a request for access to personal information. The minimal fee charged for access is intended to recover some of the actual and necessary costs incurred by the practice to provide access and it may include the costs associated with:

- locating and retrieving
- producing and copying
- preparing for disclosure
- postage or shipping costs

The fee **must not generate any profit**, and does not usually include reviewing the records to make sure the practice is complying with its obligation in PIPA to withhold information.

When charging fees, the practice must provide the applicant with a written estimate of the total fee, and may require the applicant to pay a deposit before processing the request.

It should be noted that if an employee makes the request, no fee can be charged for providing access to that person's employee personal information. "Employee personal information" is defined in PIPA as personal information about an individual that is collected, used, or disclosed solely for the purposes reasonably required to establish, manage or terminate an employment relationship. "Work product information" is excluded from the definition of personal information in PIPA so the practice does not have to disclose it to the applicant. "Work product information" means information that is prepared or collected as part of an individual's responsibilities or activities related to their employment but does not include personal information about individuals who did not prepare or collect the personal information.

Complaints About Access

The practice must educate staff on how to appropriately respond to such requests. If a patient or employee is not satisfied with the response, he or she may ask the physician's office to reconsider the response and address the complaint internally. If the complaint cannot be resolved, the practice should inform the complainant that they may contact the College of Physicians Surgeons to resolve the matter. The complainant should also be informed that they have 30 business days to make a formal complaint to the Office of the Information and Privacy Commissioner, starting from the date that the physician's office communicates to the complainant its reasons for the response (www.oipc.bc.ca).

For more information about responding to complaints, see Guidelines for Responding to Patient and Employee Complaints.

Guidelines for Secondary Use of Personal Health Information for Research

This section will:

- summarize the requirements under PIPA regarding patient consent for the use of personal health information for research purposes
- identify key considerations for physicians who wish to disclose personal health information to external health researchers

Physicians must obtain express consent for secondary uses, such as research, before using personal health information that was initially collected for clinical purposes. While express consent for the change in use from clinical to research purposes can be either written or verbal, having the patient sign a consent form is best practice.

Express consent is also required if a physician wishes to disclose personal health information to external health researchers, such as those affiliated with universities, health authorities or other health care organizations. If it is impractical to seek consent, PIPA authorizes the disclosure of personal health information without consent for research purposes if **all of the following conditions are met**:

- The research purpose cannot be accomplished unless the personal information is provided in an individually identifiable form.
- The disclosure is on condition that it will not be used to contact persons to ask them to participate in the research.

- 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.
- The organization to which the personal information is to be disclosed has signed an agreement to comply with:
    - PIPA
    - the policies and procedures relating to the confidentiality of personal information of the practice that collected the personal information
    - security and confidentiality conditions
    - a requirement to remove or destroy individual identifiers at the earliest reasonable opportunity
    - prohibition of any subsequent use or disclosure of that personal information in individually identifiable form without the express authorization of the practice that disclosed the personal information
- It is impracticable for the practice to seek the consent of the individual for the disclosure.

There is an important exception to this authorization to disclose personal health information for research purposes without consent. PIPA prohibits the disclosure of personal health information for market research purposes to drug companies or other businesses without consent.

The use of personal health information for research may require review and approval by a research ethics board. Where such review is required, the practice must refrain from disclosing personal health information for research purposes until the researcher has obtained the requisite approvals.

Best Practices

After consent from the patient is obtained, or the conditions outlined above are met, consider:

- de-identifying personal health information to whatever extent is feasible and practical before disclosing to external health researchers
- retrieving and/or securely destroying records once the research is complete
- immediately ceasing collection, use or disclosure of the personal health information unless otherwise permitted under PIPA when a patient withdraws their consent to the collection, use, or disclosure of personal health information for research purposes

If a patient believes their personal health information has been inappropriately collected, used, or disclosed for research purposes without consent, he or she may complain to the practice's privacy officer

for review and investigation. If the patient believes the matter cannot be resolved internally, the patient has the right to bring the concern to the attention of the College of Physicians and Surgeons or to the OIPC.

Guidelines for 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 PIPA a practice is expected to securely dispose of documents that contain personal information that are no longer required for legal or business/professional purposes, in order to prevent unauthorized access, inappropriate use or identity theft. The goal is to permanently destroy personal information or irreversibly erase it so that it 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 use in the practice. A service provider may be contracted to provide the record destruction services.

Industry best practices for the secure destruction of data are constantly evolving and it is generally the responsibility of all parties who handle personal information to adequately protect that personal information.

Best Practices

Best practices for the secure destruction of personal information include:

- developing and implementing a retention and secure destruction policy
- disposing of paper records securely by cross-cut shredding (do not use single-strip, continuous shredding because it is possible to reconstruct the strips)
- incinerating paper records, if practical
- disposing 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 deleting electronic information does not constitute destruction, and a wipe utility may not completely erase the information)
- ensuring machines such as photocopiers, fax machines, scanners or printers with storage capabilities are overwritten, erased, removed, or destroyed when the machines are replaced

- keeping a destruction log that includes the patient's name, time period covered by the destroyed record(s), the method of destruction and person responsible for supervising the destruction (if applicable)
- conducting audits to ensure compliance by staff and service providers and that the retention and destruction policy is effective

The Ontario OIPC and NAID 2009 Guidelines for Destruction is a useful document that provides further details on destruction practices in Canada.

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
- check their references
- insist on a signed contract

The contract for record destruction services usually covers these key points:

- clear description of:
    - the responsibilities of the service provider for the secure destruction of the records involved
    - how the service provider will collect the records from the practice
    - how the destruction will be accomplished for the records involved
    - what the methods are for secure storage of records pending destruction
- the limited timeframe upon which records will be destroyed
- upon request:
    - provision of a certificate of destruction documenting date, time, location, operator, and destruction method used
    - permission for an authorized person from the practice to visit the facility and/or witness the destruction
- request for proof of or requirement for employees receiving training on the importance of secure destruction of confidential personal information
- if the provider is subcontracting the destruction to a third party, require that notice be provided ahead of time with a contract in place with the third party that is consistent with the service provider's obligations to the practice

In order to have Canadian privacy protections apply to personal information, it is recommended that service providers operating within Canada be engaged. However, for a variety of reasons many service providers operate some or all portions of their services outside the country. 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).

For more information, see Guidelines for Confidentiality Agreements Service Contracts and Information Sharing Agreements and the BC E-waste website End-of-Life Electronic Equipment Recycling Program.

Guidelines for Use of Email or Fax

This section will:

- summarize the benefits and privacy risks associated with the use of email or fax in the clinical context
- identify key considerations for physician's offices that use email or fax to transmit personal health information

Physicians must take steps to reduce the risks associated with email or fax communications and ensure that reasonable safeguards are in place to protect personal health information.

What are the risks?

When using email or fax to transmit personal health information to patients, the following issues may negatively impact patient care:

- difficulties:
    - confirming the identity of the patient in an incoming email or fax
    - ensuring the correct recipient with only the patient's name, email address or fax number, as patients may have similar names
- risk to patients:
    - suffering adverse health consequences if it is an urgent matter and there is a delay in the response time
    - misinterpreting the content of an email or fax, which could lead to:
        - adverse health consequences
        - a complaint
        - legal action if the patient's perception is one of inadequate or ineffective communication

Using email to communicate with patients or third party health providers can give rise to the following privacy and security issues.

- An email message that is not encrypted can be:
  - intercepted by unauthorized third parties
  - altered and forwarded to unintended recipients
- Email messages containing personal information can be intercepted by unauthorized third parties if the email is:
  - delivered to the wrong address;
  - sent or received from unsecured locations such as those publicly accessible or a shared home computer;
  - retained on a home computer;
  - sent or received using a public Wi-Fi network;
  - shared by internet service providers with other third parties; or
  - saved on unsecured backup servers and subject to improper organizational retention rules.
- Attachments in an email may contain viruses that could cause serious damage to computer systems.
- The personal health information being emailed may leave Canada during transmission, and may be subject to laws in other jurisdictions that have inadequate protections or no protections at all.
- Faxing personal health information can have privacy and security risks of personal information being accessed by unauthorized third parties if the fax is:
  - sent to an incorrect fax number (caused by misdialling or by pressing the wrong speed-dial key);
  - exposed to unauthorized individuals simply because the fax machine is located in an open, unsecured location; or
  - accessed by third parties who are tapping into or monitoring the transmission.

Best Practices

Consider informing patients:

- about how emailing or faxing personal information can result in accidental disclosure or interception by other people not intended to receive the information
- what precautions the practice has taken to reduce the risks
- if the personal information is very sensitive, what other delivery options exists that are more secure (e.g., photocopies sent by mail or courier)

- that they can withdraw consent at any time to using fax or email as a method of communication, and how to do so

Office policies on use of email and fax usually include:

- criteria for the patient-provider communication, acceptable use, email etiquette, and management of email documentation as part of the patient's medical record
- staff training on the
    - appropriate use of email and fax
    - maintenance of emailed or faxed documents
- a process to remove a patient from email or fax communications if the patient withdraws consent to using any of these methods of communication
- appropriate destruction methods for emails and faxes, including deletion of emails from computer hard drive and faxes from memory

When communicating with patients or third party health care providers by email:

- Only use email systems that encrypt the email transmission and incoming and outgoing emails (or that apply other similar industry-standard protections).
- Protect each email inbox that is used to send or receive messages with a secure password known only by the individuals authorized to access the inbox.
- Protect any attached documents with a strong password and call the recipient to let them know.
- Confirm that you have the correct email address for the intended recipient.
- Verify email addresses regularly as they can be duplicated, and may frequently change.
- Whenever possible, leave sensitive personal health information out of the email or use obscure identifiers to protect it during transmission (e.g., avoid disclosing a patient's prognosis or diagnosis in an email, and instead ask them to call and make an appointment with the physician to get their results).
- Add a confidentiality disclaimer to email messages that states
    - the content is confidential and only intended for the stated recipient
    - anyone receiving the email in error must notify the sender and return or destroy the email
- For sensitive personal health information, contact the recipient by phone to inform them that confidential information is being sent and ask the recipient to call back to confirm receipt.
- Never use email distribution lists to send personal health information.

When communicating with patients or third party health care providers by fax:

- Only use fax systems that encrypt the fax transmission and incoming and outgoing faxes (or that apply other similar industry-standard protections).
- Protect the fax machine or the fax modem (a fax device that uses a computer program) with a secure password known only by individuals in the office who are authorized to send or receive faxes.
- Ensure the fax machine is located in a secure area in your practice to prevent unauthorized persons from viewing or receiving the documents.
- 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.
- Whenever possible, leave sensitive personal information out of the fax or use obscure identifiers to protect it during transmission
- Include a disclaimer stating
    - the faxed material is confidential and only intended for the stated recipient
    - anyone receiving the fax in error must immediately notify the sender and return or destroy the fax
- Before faxing the information, confirm the recipient's fax number (including when using a pre-programmed number) and confirm that the personal health information will be protected upon receipt
- If using pre-programmed fax numbers, regularly verify these numbers for accuracy
- 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
- Check each day's fax history report for errors or unauthorized faxing
- When receiving faxes
    - retrieve documents sent by fax as soon as they have been processed
    - do not leave the documents sitting on or near the fax machine
    - if a fax is received in error, promptly notify the sender and return or destroy the information

Sharing fax machines with other offices is discouraged, particularly where personal information is frequently sent and received.

Although PIPA does not require it, a best practice is to avoid the disclosure of personal health information outside of Canada and prohibit access to such records from outside Canada without express patient consent.

Retention of Emails or Fax Documents

For storage and retention of emails and faxes, consider the following:

- Do not make or retain more copies of email communications than needed.
- Securely destroy extra copies that are no longer needed.
- Include personal health information that is emailed as part of the patient's medical record.

For additional information on emailing personal health information, see Emailing Patient Information.

Guidelines for Use of Mobile Devices

This section will:

- summarize the risks and benefits of using mobile devices to provide health care services
- identify key requirements and best practices for using mobile devices

Mobile devices such as smartphones and tablets allow a physician convenient and timely access to patients and other health care providers remotely. However, the use of mobile devices in a practice can create privacy and security risks to personal information. Those risks include loss or theft of the device, malicious programs that track or spy on the device and having personal information be intercepted or monitored by unauthorized third parties. Any wireless device, including a mobile device, that is connected to a network (e.g., Wi-Fi, Bluetooth, 3G and near-field communication) can serve as an illicit entry point to the entire network if it is not properly set up with appropriate security controls.

Best Practices

Physicians have an obligation to ensure adequate administrative, physical and technical safeguards are in place before using mobile devices in their practice. This obligation extends to staff and third parties who have access to personal information under the practice's custody or control. Physicians must also take reasonable steps to ensure any devices, apps or programs used by their practice comply with PIPA.

- Ensure:
    - devices have strong, up-to-date, industry-standard encryption for transmitting personal information to minimize the risk of unauthorized interception
    - devices are protected with a secure password that is at least six characters long with a combination of numbers, upper and lower case letters
    - anti-malware software is installed and up to date to protect against attacks
    - any systems to which the device is connected provides adequate end-to-end security
    - any cloud services used to transmit or store data are secure and use encryption (do not use public services that can be easily accessed by unauthorized third parties)

  - voice command features are disabled if they are not needed, as this feature allows the device to always be listening
  - the screen is set to lock automatically after a short period of inactivity
- Never:
  - use public Wi-Fi connections as they are vulnerable to unauthorized interception
  - "jailbreak" or root the device as this weakens its security
- Limit:
  - the number of incorrect password attempts before the data is deleted
  - access permissions for apps, unless the permissions are related to the service
  - location information used by programs to avoid creating a log of your movements, which may include visits to patients' homes
- Always:
  - use apps that come from official app stores and that use strong, up-to-date, industry-standard encryption
  - keep software up to date
- Promptly report a lost or stolen device, and consider using programs that help you locate your phone.
- When returning or disposing of a device, ensure it is completely wiped and safely disposed of.
- Delete personal information from the device once it's been added to the patient's medical record.

It is recommended that policies regarding the use of mobile devices in a practice be included in the practice's privacy management program.

For more information on mobile devices and privacy, see

- Top 15 Tips: Mobile Devices: Tips for Security and Privacy
- Contemplating a Bring Your Own Device (BYOD) Program? Consider These Tips

Privacy Resources for Physicians

BC Privacy Legislation	
BC e-Health Act News Release	http://www2.news.gov.bc.ca/news_releases_2005-2009/2008HEALTH0038-000505.htm
Freedom of Information and	http://www.qp.gov.bc.ca/statreg/stat/F/96165_01.htm

Protection of Privacy Act	
Guide to the Personal Information Protection Act	https://www.oipc.bc.ca/guidance-documents/1438
Personal Information Protection Act	http://www.qp.gov.bc.ca/statreg/stat/P/03063_01.htm
Codes of Ethics and Privacy	
CMA Code of Ethics	https://www.cma.ca/En/Pages/code-of-ethics.aspx
CMA Privacy and Confidentiality	https://www.cma.ca/En/Pages/privacy-confidentiality.aspx
Principles for the Protection of Patients' Personal Health Information	http://policybase.cma.ca/dbtw-wpd/Policypdf/PD11-03.pdf
Accountability	
Electronic Records Handbook	https://www.cmpa-acpm.ca/documents/10179/24937/com_electronic_records_handbook-e.pdf
Leaving Practice	https://www.cpsbc.ca/files/pdf/PSG-Leaving-Practice.pdf
Medical Records – Issues & Guidelines	https://www.divisionsbc.ca/provincial/patientdataagreement
Medical Records Standards	https://www.cpsbc.ca/files/pdf/PSG-Medical-Records.pdf
Telemedicine in Primary Care Policy Statement	https://www.doctorsofbc.ca/sites/default/files/final-telemedicine-in-primary-care-policy-statement.pdf
Telemedicine Standards	https://www.cpsbc.ca/files/pdf/PSG-Telemedicine.pdf
Data Handling	
Consent: A Guide for Canadian Physicians	https://www.cmpa-acpm.ca/en/handbooks/-/asset_publisher/TayXf91AzWR2/content/consent-a-guide-for-canadian-physicians
Disclosure of Patient Information to Law Enforcement Authorities	https://www.cpsbc.ca/files/pdf/PSG-Disclosure-of-Patient-Information.pdf
Emailing Patient Information	https://www.cpsbc.ca/files/pdf/PSG-Emailing-Patient-Information.pdf

Email and Legal Risks	https://www.cmpa-acpm.ca/-/using-email-communication-with-your-patients-legal-ris-1
Fax and Preventing Privacy Breaches	https://www.cmpa-acpm.ca/en/safety/-/asset_publisher/N6oEDMrzRbCC/content/10-ways-physicians-can-prevent-privacy-breaches-when-using-fax-with-other-healthcare-professionals
Photographic, Video and Audio Recording of Patients	https://www.cpsbc.ca/files/pdf/PSG-Photographic-Video-Audio-Recording.pdf
Privacy Breaches: Tools and Resources	https://www.oipc.bc.ca/guidance-documents/1428
Protecting Personal Information	http://www2.gov.bc.ca/gov/content/employment-business/business/managing-a-business/protect-personal-information
Protecting Personal Information Away from the Office	https://www.oipc.bc.ca/guidance-documents/1447
Securing Personal Information: A Self-Assessment Tool for Organizations	https://www.oipc.bc.ca/guidance-documents/1439
Information Technology	
Cloud Computing for Small- and Medium-Sized Enterprises	https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/online-privacy/cloud-computing/gd_cc_201206/
Contemplating a Bring your Own Device (BYOD) Program? Consider These Tips	https://www.oipc.bc.ca/guidance-documents/1828
Doctors Technology Office Technical Bulletins	https://www.doctorsofbc.ca/technical-bulletins
Getting IT Right	https://www.doctorsofbc.ca/sites/default/files/gettingitright.pdf
Health Information Standards	https://www.infoway-inforoute.ca/en/component/content/article?id=231
Physician Office IT Security Guide	https://www.doctorsofbc.ca/resource-centre/physicians/managing-practice/technology
Privacy and Cybersecurity	https://www.priv.gc.ca/en/opc-actions-and-

	decisions/research/explore-privacy-research/2014/cs_201412/
Privacy in a Wired World – Protecting Patient Information	https://www.cmpa-acpm.ca/en/duties-and-responsibilities/-/asset_publisher/bFaUiyQG069N/content/privacy-and-a-wired-world-protecting-patient-health-information
Technology Unleashed – The Evolution of Online Communication	https://www.cmpa-acpm.ca/en/-/technology-unleashed-the-evolution-of-online-communication
Telemedicine Challenges and Obligations	https://www.cmpa-acpm.ca/en/advice-publications/browse-articles/2013/telemedicine-challenges-and-obligations
Telemedicine White Paper	https://www.divisionsbc.ca/CMSMedia/Divisions/DivisionCatalog-vancouver/VDoFP_Telemedicine_Nov3.pdf
Top 15 Tips: Mobile Devices: Tips for Security and Privacy	https://www.oipc.bc.ca/guidance-documents/1994
Videoconferencing consultation: When is it the right choice?	https://www.cmpa-acpm.ca/en/advice-publications/browse-articles/2015/videoconferencing-consultation-when-is-it-the-right-choice
Practice Continuity During a Disaster	
Emergency Response	https://www.divisionsbc.ca/victoria/emergencyresponse
What community physicians could offer during a disaster	http://www.bcmj.org/council-health-promotion/what-community-physicians-could-offer-during-disaster
Privacy Commissioners	
British Columbia	https://www.oipc.bc.ca
Canada	https://www.priv.gc.ca

DEFINITIONS

Access

The ability to view or collect data, particularly from an electronic database. When a record is accessed, it is usually considered a disclosure by the practice. Only authorized users should be able to access personal information in an EMR.

Application Service Provider (ASP)

A third party service provider that manages and stores the Electronic Medical Record (EMR) at its data centre, rather than the physician managing and running servers in their own practice. Physicians or their authorized employees have access to the EMR over the Internet or preferably over a private network.

Authentication

A method designed to allow a computer application to verify credentials—usually in the form of a user name and password for single-factor authentication or user name and password plus an access token for multi-factor authentication.

Canada Health Infoway

Canada Health Infoway is an independent, not-for-profit organization funded by the federal government and established in 2001. Canada Health Infoway invests funds and works with partners to accelerate the development, adoption and effective use of digital health solutions across Canada, including implementing an interoperable Electronic Health Record (EHR) system. Canada Health Infoway is accountable to its Board of Directors and the Corporation Members. The Corporation Members are made up of the deputy ministers of health for the 10 provinces, three territories and the federal government.

Circle of Care

Two or more health care providers that are delivering services to the same individual. Those health care providers have implied consent to share information with each other, unless the individual has expressly withheld or withdrawn consent. Health care providers in the circle of care can include organizations that have diagnostic information and professional case consultation information about the patient and share them with the patient's other health care providers. The circle of care should be obvious to the patient and reflect common practices. "Circle of care" is a term that is used in provincial health information legislation outside of BC, but does not exist in PIPA, where direct patient care is based on "implied consent". See also "Implied Consent".

Collection

The act of gathering, receiving, accessing or obtaining personal information.

Confidentiality

In the health care context, it refers to a physician's or other health professionals' ethical and legal obligations to protect an individual's personal health information, unless the individual consents to the disclosure or the disclosure is otherwise authorized.

Consent

The authority that an organization usually needs under PIPA to collect, use or disclose an individual's personal information. A patient can provide express or implied consent. Implied consent can be "opt-out" or "deemed". In limited circumstances, PIPA authorizes the collection, use and disclosure of personal information without consent. Consent must be voluntary, and the physician must be able to show that a reasonable person would consider the purpose for which the information is collected, used or disclosed to be appropriate in the circumstances. When providing health care services to a patient, a physician cannot require the patient to consent to the collection, use or disclosure of personal information beyond what is necessary to provide those services. An individual has the right to withdraw or change their consent by giving reasonable notice, and the physician must explain the consequences on the provision of care. See also "Express Consent" and "Implied Consent".

Data Masking

The process of restricting access to data in an electronic record by substituting real values with random characters that obfuscate or disguise the data. Data Masking can be applied at different levels of granularity depending on the unique circumstances and system capabilities.

Data Stewardship

Also known as accountability, the legal, ethical and fiduciary responsibilities of a physician in managing and protecting personal health information including collection, use, disclosure and retention.

Disclosure

Sharing, exposing or providing access to information, including to another organization, third party or to the individual the information is about.

Disclosure Directive

A written instruction from an individual to mask their Personal Health Information contained in a specific Health Information Bank (HIB), restricting access to that information under the E-Health Act. Health care

providers must obtain that individual's express consent to access the personal information, unless an emergency occurs, or other exceptions apply.

E-Health Act

Also known as the Personal Health Information Access and Protection of Privacy Act. Legislation introduced in 2008, it authorizes data flows, imposes specific privacy and security obligations for personal health information, and enhances openness and transparency regarding the sharing of information in the health sector. The E-Health Act applies only to those databases of the Ministry of Health and health authorities that have been designated as HIBs by the Minister of Health. The databases that have been designated as HIBs are the Provincial Laboratory Information Solution, the Client Registry/Enterprise Master Patient Index and the Provider Registry.

Electronic Health Record (EHR)

An electronic record system that contains personal information collected in the delivery of various health care services. Health authorities have their own EHR and there are also provincial and inter-jurisdictional EHRs, including Panorama, a public health information system. The personal information contained in an EHR system is available electronically to authorized users of the system.

Electronic Medical Record (EMR)

An electronic record system within a practice that enables a health care professional, such as a family physician, to record and store the information collected during a patient's visit instead of, or in addition to, a paper file. The EMR may also allow the physician to access personal health information from other electronic health record systems.

Electronic Medical Record (EMR) Vendor

A third party service provider that sells and supports Electronic Medical Record (EMR) software.

Encryption

The process of protecting personal information by encoding data into an electronic form that can only be read by the intended authorized recipient. All personal information of a sensitive nature should generally be encrypted.

Express Consent

A type of consent that occurs when an individual provides verbal or written agreement to the collection, use or disclosure of their personal information, after being informed about the type of personal information being consented to, and the purposes for which the information is being collected, used or disclosed. Express consent can be verbal or written, though it is easier to prove that consent was given if it is provided in writing. Consent to the collection, use or disclosure of personal information cannot be a condition of providing health services, beyond what is necessary to provide those health services.

Freedom of Information and Protection of Privacy Act (FIPPA)

BC privacy legislation that governs how personal information is collected, used, disclosed and protected by public bodies, including health authorities and the Ministry of Health.

Health Authority

Includes the following entities that deliver health care services to British Columbians:

- Provincial Health Services Authority
- five regional health authorities:
  - Fraser Health
  - Interior Health
  - Northern Health
  - Vancouver Coastal Health
  - Vancouver Island Health
- First Nations Health Authority
- Providence Health Care

All personal health information collected, used and disclosed by the health authorities is governed by FIPPA with the exception of the First Nations Health Authority which is governed by PIPA. This toolkit uses the term to refer to the health authorities that are governed by FIPPA.

Health Information Bank (HIB)

An electronic database under the custody and control of the Ministry of Health or a health authority that contains personal health information and is designated by the Minister of Health under the E-Health Act

as a HIB. The designation order authorizes specific data flows and establishes the privacy and security framework for the HIB.

Implied Consent

An individual's implied agreement to the collection, use or disclosure of their personal information by an organization that takes the form of either opt-out consent or deemed consent. Opt-out consent (see s. 8(3) of PIPA) is a form of implied consent that occurs when an individual receives notice, in a manner the individual can reasonably be expected to understand, that their personal information will be collected, used or disclosed for a specific purpose. The individual must also be provided with a reasonable amount of time to decline after being informed. The collection, use or disclosure must be reasonable, having regard to the sensitivity of the information in the circumstances, and must be limited to the purpose set out in the notice. Deemed consent (see s.8(1) of PIPA) is the second form of implied consent, where an individual volunteers information for a purpose that is obvious, and a reasonable person would think that it was appropriate for the individual to volunteer that information in the circumstances.

Information-Sharing Agreement (ISA)

A written agreement that sets out the terms and conditions for the collection, use and disclosure of personal information by an organization or public body from or to an individual or third party (such as a service provider). An ISA should generally include the specific purpose of the agreement, a description of the personal information covered by the agreement and how it will be collected, used and disclosed, any conditions or limitations on the collection, use and disclosure and information on maintaining the accuracy of the personal information, the security arrangements employed and how compliance with the agreement will be monitored and reviewed. Public bodies have specific requirements for ISAs in s. 69 of FIPPA, and information in a health information bank may only be disclosed if the ISA requirements in s. 19 of the E-Health Act are met.

Mobile Device

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

"Need to Know" and "Least Privilege" Principles

The “need to know” principle states that authorized users of a system should only have access to the minimum amount of personal information that is necessary to perform their duties within a public body or an organization. The “least privilege” principle requires that each authorized user in a system be granted the most restrictive access privileges needed for performing authorized tasks. The principles are reflected in privacy law but not always expressly stated.

Personal Health Information

Information about an individual that is collected, used or disclosed as part of a medical record for the purpose of delivering health services to that individual. In the E-Health Act, personal health information is defined as “recorded information about an identifiable individual that is related to the individual's health or 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, personal address, birth date, physical description, medical history, gender, education, employment and visual images such as photographs or videotapes.

Personal Information Protection Act (PIPA)

BC privacy legislation that governs how personal information is collected, used, r disclosed, and protected by private sector organizations, including physicians’ private practices and other private health care facilities.

Personal Information Protection and Electronic Documents Act (PIPEDA)

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, influence or interruption and to control one’s personal information. It is linked with other fundamental rights such as freedom of expression, security of the person, dignity and personal autonomy. Privacy also includes the right of individuals to determine when, how and to what extent they share information about themselves with others.

Privacy Breach

Unauthorized access, collection, use, disclosure, or disposal of personal information.

Privacy Impact Assessment (PIA)

An assessment tool/process that identifies the privacy risks of a proposed initiative involving the collection, use or disclosure of personal information and the steps that will be taken to mitigate those risks.

Privacy Management Program

A program that demonstrates an organization's accountability for personal information and capacity to comply with applicable privacy laws and related industry standards, as well as correctly identifying, addressing or minimizing privacy-related obligations and risks. Includes appointing a privacy officer, responding to requests for access and complaints under PIPA, and developing, implementing, maintaining and updating policies, systems, procedures and training for collection, use, disclosure, consent, notification, access to information, retention, disposal, privacy breaches and corrections. See also "Privacy Officer".

Privacy Officer

The individual designated to be accountable for ensuring organizational compliance with privacy legislation, industry standards for privacy and privacy-related professional and regulatory obligations. In a medical practice, one physician must be designated as the privacy officer. If it is a solo practice, the solo physician is the de facto privacy officer. The responsible physician may choose to delegate responsibilities for the privacy management program to an employee but they remain ultimately responsible.

The privacy officer is responsible for

- developing policies and procedures
- implementing program controls
- designing and implementing employee training and education
- conducting ongoing assessments and revising program controls
- monitoring for compliance
- managing privacy breach incidents

- managing complaints
- answering questions
- responding to requests for access to or correction of personal information
- demonstrating leadership in creating and maintaining a culture of privacy
- being informed of any privacy related changes in legislation

Private Network

A secure, private, end-to-end network that allows secure, high-speed access to an EMR or an EHR, secure Internet access and secure email messaging.

Reasonable Security Measures

The measures taken to protect personal information from unauthorized collection, use or disclosure by implementing physical controls (e.g., locked cabinets, securely stored laptops or key card access), technical controls (e.g., firewall, document encryption or user access profiles) and administrative controls (staff training, privacy policy or retention and destruction policy). Factors to consider when implementing reasonable measures include the sensitivity of the personal information (medical records are considered highly sensitive), the likelihood of a privacy breach, the harm caused if a breach occurred, the type of record involved, the cost of the security measures and current industry standards.

Remote Access

The ability to get secure access to a computer or network from outside the practice. Individuals who are travelling or working from home may need access to information and may access the network and systems remotely.

Role-Based Access

A policy and technical architecture involving the assignment of access privileges to roles based on job functions rather than to individual users. Users are granted privileges in accordance with the "need to know" and "least privilege" principles by virtue of being authorized to act in specific roles.

Security

Controls that protect personal information from unauthorized collection, use or disclosure. Examples include locking cabinets, or in relation to electronic records, password protections, encryption and firewalls. See also "Reasonable Security Measures".

Staff

May include employees, 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 or random such that it is 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 one or more numbers, upper and lower case letters and symbols (e.g., IloveParis!936).

Third Party

In the context of personal information that is controlled by a practice, refers to anyone outside the practice or the individual the information is about.

Two Factor Authentication

The combination of user name/password (something an authorized user knows) and some other physical identification tool like a secure ID token (something an authorized user has), which are both required in order to verify the identity of a person.

Use

Any operation (other than collection or disclosure) performed on, or use made of, personal information by the practice or third party that collected the information for a specified purpose.

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 method that allows connection from outside the practice to the EMR over the Internet with enhanced security.