May 2025

A Privacy Management Handbook for Small Health Care Organizations

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Welcome to the IPC's Privacy Management Handbook for Small Health Care Organizations

Whether you're an individual health professional or operating a small group practice or clinic, this guide will help you develop a privacy management program and meet your obligations under PHIPA.

Contents

Purpose

The purpose of this handbook is to provide individual health practitioners and other small health care organizations with a useful reference for building an effective privacy management program.

Using this handbook may help them identify potential gaps or weaknesses in their information practices that could be strengthened to better protect their patients' personal health information.

This handbook (including appendices) summarizes basic requirements and best practices under the *Personal Health Information Protection Act* for general informational purposes only. It should not be relied upon as a substitute for the legislation itself and is not legal advice. It is not binding on the IPC's tribunal, which may be called upon to independently investigate and decide upon a privacy or access complaint based on the specific facts and unique circumstances of a given case. For the most up-to-date version of this guidance, please visit **www.ipc.on.ca.**

In developing this guidance, the IPC consulted with a number of health practitioners, health privacy experts, health-related associations, and select members of the IPC's Strategic Advisory Council on an earlier draft. The IPC is grateful for the feedback we received.

1.0 Introduction

In today's digital world, safeguarding personal health information is more important than ever. That's why good information practices as part of a robust privacy management program are essential. It goes beyond complying with privacy laws – it's about protecting your patients' personal health information and securing their trust in you.

1.1 About this handbook

Privacy is paramount

Compliance with *Ontario's Personal Health Information Protection Act* (PHIPA) is essential for ensuring individual rights and protections, but navigating legislation can be confusing and overwhelming for individual practitioners and small health care organizations. Our intention with this handbook is to help clarify your obligations when it comes to protecting personal health information and help you set up a privacy management framework for your practice.

Giving you tips and tools for success

In the handbook, we provide:

- information on what you need to do to meet PHIPA requirements
- tips and guidance to help you build a privacy management program that's right-sized for your practice
- additional resources that may be useful if you'd like more details

Ultimately, building good privacy management practices that demonstrate both compliance with PHIPA and care for your patients is essential for success. Since we don't expect busy health care practitioners to be privacy experts, our goal is to provide you with basic knowledge about the practical steps you should be taking to meet your privacy obligations. Throughout this document, we use plain, easy-to-understand language to keep the information simple. In short, we've created reader-friendly content for the busy health practitioner who's a non-privacy specialist. We hope you find the handbook useful in building or strengthening your privacy management program.

Who is the handbook for?

This handbook is designed primarily for custodians that are:

- sole practitioners who independently own and operate their own health care practice
- small group clinics that provide similar or interdisciplinary health care services
- operators of small health care facilities

Examples of custodians might include doctors, nurses, audiologists and speech-language pathologists, chiropractors, chiropodists, dental professionals, dieticians, massage therapists, midwives, optometrists, occupational therapists, opticians, pharmacists, physiotherapists, psychologists, and respiratory therapists.

Whether you operate as sole practitioners, or as members of small health care facilities, such as family practice groups, specialist clinics, walk-in clinics or community-health centres, this handbook may be relevant to you.

In all cases, if you're a provider of health care, it is important to determine your status as custodians or agents under the law. This is explained further in this handbook.

The IPC is here to help

In addition to this handbook, the IPC has created a variety of resources to help health care organizations and practitioners better understand their privacy obligations and how to safeguard personal health information. These resources include a variety of guidance materials — from factsheets to podcasts and video presentations. They are all available on the IPC's website at **www.ipc.on.ca**.

For a list of suggested resources, see Appendix 4.

Understanding key terms

To understand this handbook, it is important to clarify certain key terms from the outset.

Who is a health information custodian?

Under PHIPA, a health information custodian (custodian) is generally a person or an organization that provides health care to individuals and has custody or control of their personal health information. As a first step, it's important to determine if you are considered a custodian since, as a custodian, you are ultimately accountable for ensuring compliance with PHIPA.

Custodians include health care practitioners who are members of a regulated health care profession or the Ontario College of Social Workers and Social Service Workers who provide health care, or any other person whose primary function is to provide health care for payment.

Custodians also include operators of any of the following facilities, programs or services:

- hospitals, psychiatric facilities or integrated community health services centres
- long-term care homes, retirement homes or care homes
- pharmacies
- laboratories or specimen collection centres
- ambulance services
- homes for special care
- centres, programs or services for community health or mental health whose primary purpose is the provision of health care

In some cases, custodians may be employed to provide health care on behalf of organizations that are not themselves custodians under PHIPA. For example, a nurse employed by a school board; a doctor employed by a professional sports team; a registered massage therapist providing health care to clients of a private health spa; or a nurse employed in-house by a manufacturing firm.

Who is an agent?

A custodian may authorize an agent to collect, use, retain, disclose or dispose of personal health information for them, or on their behalf. Agents have certain responsibilities of their own under PHIPA. It is important to note, however, that custodians remain accountable for the actions of their agents whether or not the agent has the authority to bind the custodian, is employed by the custodian or is being remunerated. Agents are often employees but might also be volunteers or contractors.

Conversely, employees whose job does not involve working with personal health information on behalf of the custodian would not be agents. Throughout this handbook, we will use the term employees to refer to any full and part-time staff, contractors, or volunteers. The term agent will be used specifically for team members who handle personal health information on the custodian's behalf.

If you are unsure about whether you are a custodian or an agent under PHIPA, contact your professional association or regulatory college for guidance. You can also review other guidance published by the Office of the Information and Privacy Commissioner of Ontario on our **website** to help you understand your role and your obligations.

What is personal health information?

It is important to understand what personal health information is under PHIPA, since PHIPA does not apply to just any information.

Personal health information under PHIPA means identifying information about an individual in oral or recorded form, if the information:

- relates to the individual's physical or mental condition, including family medical history
- relates to the provision of health care to the individual
- is a plan that sets out home and community care services to be provided for the individual
- relates to payments, or eligibility for health care or for coverage for health care
- relates to the donation of any body part or bodily substance or is derived from the testing or examination of any such body part or bodily substance
- is the individual's health number
- identifies a health care provider or a substitute decision-maker for the individual

Identifying information includes information that identifies an individual or information that can reasonably foreseeably be used, either alone or with other information, to identify an individual. The definition of personal health information also includes other identifying information that is contained in a record that contains personal health information.

1.2 Why privacy matters to your practice and patients

Health care is rapidly changing in Ontario. For example:

- virtual services are increasingly being offered in addition to in-person visits
- multi-disciplinary and community-based models are providing more holistic, patient-centred care
- new digital apps and technologies are being offered off the shelf, and more

Amid these transformative changes, health data is being used and shared more than ever to support the delivery of modern and effective health care.

Additionally, we are living in a whole new digital world. While every click promises something new and exciting, dangerous threats may be hiding online. Cybercrime continues to grow exponentially in all sectors, including the health sector where an increasing amount of health information now exists online, in the cloud and in third party systems. Cyberattacks can lead to serious harms, including leaked confidential records, lost access to records, and the disruption of systems and services. For smaller health organizations, cyberattacks can be particularly crippling.

Read about what happened to a medical imaging clinic that was the subject of a ransom attack and some practical lessons learned in Ransomware reality: Case study in health care cybersecurity and recovery

In the face of such changes and threats, it's critical that health care practitioners understand their privacy obligations and uphold their commitments to their patients. Today's health practitioners must be more vigilant than ever to respect patient confidentiality and keep personal health information secure. These are fundamental conditions for earning and keeping patient trust. Patients provide their personal health information when seeking medical care because they trust their health care provider will protect their privacy.

Without trust, patients may refrain from offering that information. Or they may be less forthcoming about their symptoms or less truthful about following treatment plans. They may also be hesitant to adopt new digital solutions, participate in research, or allow their personal health information to be shared for broader public health purposes. Worse still, they may avoid seeking help altogether. As the old adage goes, "Trust takes years to build, only seconds to break, and forever to repair."

1.3 Ontario's PHIPA and how it impacts you

Privacy is a fundamental right of every Ontarian. To respect that right, health information custodians are required by law to protect personal health information, and to follow the rules set out under PHIPA when collecting, using, and disclosing that information.

PHIPA governs the collection, use, and disclosure of personal health information within the health sector. Regulated health professionals and other health information custodians in Ontario must comply with PHIPA. The role of the Information and Privacy Commissioner of Ontario (IPC) is to

oversee compliance with PHIPA to ensure that Ontario's custodians — as well as other persons, organizations, and entities subject to PHIPA — abide by the privacy principles and requirements set out in the law.

In this handbook, we focus on things that small health information custodians should be thinking about and doing to build or strengthen a privacy program in compliance with PHIPA requirements.

PHIPA balances the privacy rights of individuals with the legitimate need of custodians to collect, use, and disclose personal health information for the delivery of effective and timely health care.

Your patients have the right to:

- **Be informed about …**
  - why you need to collect, use, and/or disclose their personal health information
  - any theft, loss, or unauthorized use or disclosure of their personal health information
  - their right to refuse or withdraw their consent to the collection, use, or disclosure of their personal health information, except in certain circumstances
- **Make requests …**
  - to access a copy of their records of personal health information, subject to certain exceptions
  - to have corrections made to their records of personal health information, subject to certain exceptions
- **Complain to the IPC if they are …**
  - refused access or where the custodian is deemed to have refused access to their personal health information
  - refused a correction request or where the custodian is deemed to have refused a correction request
  - concerned about a privacy breach or potential breach

As a health information custodian, you may, under certain conditions:

- **Collect personal health information …**
  - that is necessary to provide your patient with health care
- **Use personal health information …**
  - for risk or error management to improve the quality of care you provide your patients
  - for the purpose of obtaining payment for provision of health care (billing)
  - for educating your agents to provide health care
- **Share personal health information …**
  - for purposes of research
  - to an auditor or a person conducting an accreditation review

- to help support the evaluation, planning, and management of the health system
- to help improve the provision of health care

- For more information, see our short, educational **IPC FYI Health Privacy videos** that help explain it in simple terms

Sharing personal health information for broader health purposes

As a health care provider, the primary purpose for which you collect, use, or disclose personal health information is to provide health care to your patients. However, it's important to know that as long as certain requirements are satisfied, PHIPA also allows personal health information to be used or disclosed outside the direct patient-provider relationship — even without consent — so that it can be used to help to improve the health care system and the health of the general public. These uses and disclosures are allowed because PHIPA recognizes that the responsible sharing of personal health information for the right reasons can benefit the public and improve health care for everyone.

PHIPA permits the use and disclosure of personal health information for the following purposes, provided that specified requirements are satisfied.

- conducting research
- planning, evaluating, and managing the health system
- maintaining a registry of personal health information to improve the provision of health care
- protecting and promoting public health

For more information about the various ways in which personal health information can be used or disclosed for these purposes and the conditions that must be met to do so, please refer to the IPC's guidance document **Use and Disclosure of Personal Health Information for Broader Public Health Purposes**.

1.4 What is a privacy management program?

Make privacy your business as usual!

When people entrust you with their personal health information, they expect it to be handled securely and responsibly.

A privacy management program is a combination of the policies, processes, and actions that you can use to protect personal health information, comply with requirements under PHIPA, and build trust with patients. Creating a privacy management program will help you achieve the privacy standards that patients expect of you and demonstrate your commitment to keep doing so. In fact, it's an essential activity for any modern organization today.

Establishing a privacy management program is never a one-and-done thing. Your privacy management program needs to be further developed as you mature as an organization and gain more privacy knowledge and sophistication. This will strengthen the robustness of your information governance practices over time and demonstrate that you are taking reasonable steps to comply with PHIPA.

Respecting patient privacy is about effectively managing the personal health information you hold and keeping it safe. It's about robust information stewardship and showing patients and all your stakeholders that you have good practices in place

Determine what's needed for your practice

There is no one-size-fits-all solution to developing a privacy program. As practitioners, you will need to determine, taking into consideration your organization's size and situation, what is relevant to your practice and how best to apply the guidance in this handbook.

The business case: Benefits of a privacy management program	
	**Enhance information management and protection** Through a well-managed privacy management program, you can establish strong privacy and security practices that enhance protection of your health data.
	**Meet patient expectations and increase their trust** People today are more sensitive than ever about how their personal health information is handled. Having a strong privacy management program in place will signal to your clients that you are committed to protecting their privacy as a top priority.
	**Reduce your risk** Implementing a robust privacy management program will reduce the risk of cyberattacks and privacy breaches, along with the resulting reputational damage, financial costs and lost time and business.
	**Stand out as a leader in your community** Don't view privacy as an obligation—treat it as a differentiator! A good privacy program signals that you care for patient interests and distinguishes you as a leader in your community. Plus, more partners and suppliers want to do business with privacy-minded professionals and organizations.
	**Regulatory compliance** With stricter regulations around privacy, creating a privacy management program that encompasses the necessary policies and practices can help you meet your responsibilities under PHIPA and avoid the consequences of non-compliance.

1.5 Let's get started

Developing a privacy management program may sound intimidating but it doesn't have to be. This handbook takes you through the process of creating, maintaining, and following a program that will work for you and your practice. Read on for simple tips and information designed to make your privacy journey as easy and as straightforward as possible.

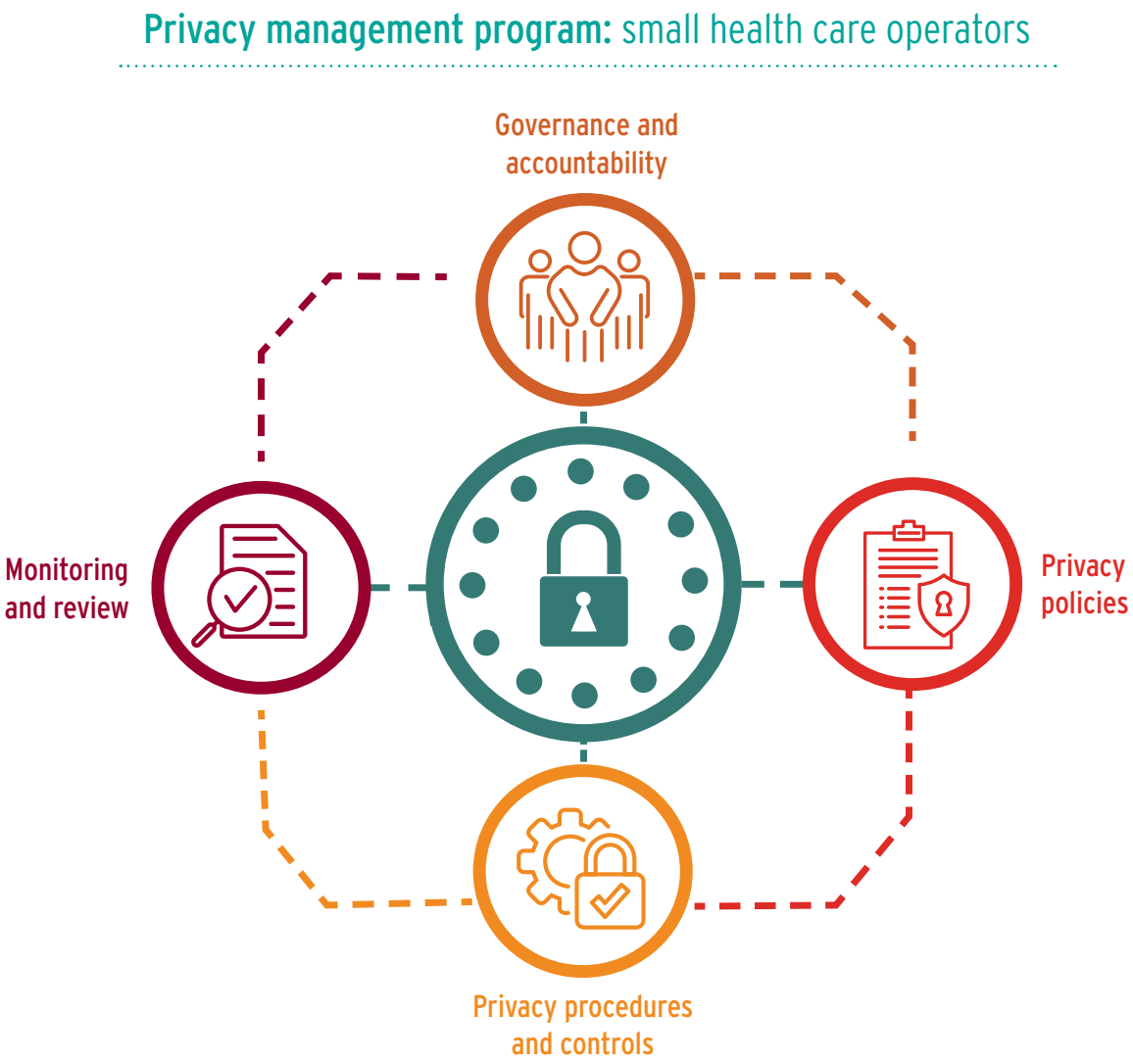
Don't expect to build a privacy program in a day, or a week! The process will, of course, depend on the size of your practice and the time you can devote. It's a journey: tackle it in steps and use this handbook as a guide.

Initial components of a privacy management program for small health care organizations

Constructing a solid privacy management program takes careful planning and consideration. While there are many elements to a privacy program, there are four main parts to consider:

1. **Governance and accountability:** create a solid foundation for your program by clearly assigning roles and responsibilities so that nothing falls between the cracks
2. **Privacy policies:** are the written rules that you and your employees commit to following so that everyone clearly understands what is expected of them
3. **Privacy procedures and controls:** help you operationalize your policies in practice to make them real
4. **Monitoring and review:** are the means by which you continually assess the effectiveness of your program and make improvements to it over time.

Each of these components are described further in this handbook.



DEVELOPING YOUR PRIVACY PROGRAM

2.0 Governance and accountability: Creating the foundation

A strong privacy management program starts with governance and accountability. It's about taking a comprehensive, structured approach to assigning roles and responsibilities and integrating a culture of privacy protection at the core of your operations.

2.1 Tone from the top

Make data protection part of your organizational culture

To be effective in protecting personal health information, your organization's approach to privacy needs to be more than words on a page. Fostering a culture that prioritizes privacy and security starts with leadership and commitment from the highest levels of the organization, whether tall or flat, so that day-to-day practices always reflect key privacy principles.

Here are three core privacy principles that should permeate throughout your organization:

1. You should only collect, use, or disclose personal health information with consent, unless PHIPA permits or authorizes you to do otherwise.
2. You should not collect, use, or disclose personal health information if the information you already have meets your purpose.
3. Only collect, use, or disclose the minimum amount of personal health information that is reasonably necessary for your purpose.

Embed these core principles into your policies. Operationalize them through carefully considered procedures and practices. Ensure they are respected through effective training and ongoing monitoring and review. All these building blocks will mutually reinforce a strong privacy culture and help ensure that your patients' personal health information is protected.

2.2 Accountability is key!

Define responsibilities: Who's in charge of data protection?

Whether you're a one-person practice, a multidisciplinary health clinic, or a small hospital, accountability is key to creating the right foundation for your privacy management program. Accepting accountability means taking responsibility for protecting personal health information.

The first step is to establish who's in charge of your privacy management program. Everyone in the organization plays an important part in implementing the program but it takes a senior person to oversee it on a day-to-day basis. Clarifying roles and responsibilities among the members of your team will help ensure the success of your privacy efforts.

The person responsible for overseeing implementation of the privacy management program will depend on the size of your organization. In the case of sole practitioners or small healthcare teams, the owner of the practice might take on the role of directly overseeing the privacy management program. In larger-sized medical clinics, you might appoint a specific individual to take on this role either on a full-time or part-time basis. Typically, this role is referred to as a privacy officer.

What's a privacy officer?

The privacy officer of an organization is basically tasked with developing and operationalizing the privacy management program on a day-to-day basis and ensuring compliance with PHIPA. There are alternate job titles that can be used instead of privacy officer, such as privacy manager or privacy designate, but they essentially have the same function.

As custodians, you must designate someone (either yourself or someone on your team) to serve as a privacy officer for your organization.

A dedicated privacy officer performs a variety of functions, which may include:

- Identifying the most relevant privacy issues, risks, and opportunities for your organization
- Communicating with management on privacy related matters
- Facilitating your organization's compliance with PHIPA
- Maintaining an inventory of all personal health information that is collected, used, and shared with others
- Developing privacy and security policies and procedures and ensuring they are kept up to date
- Training employees to ensure they are familiar with, and implement, their privacy obligations
- Acting as the primary point of contact on privacy issues
- Handling privacy-related questions and complaints
- Respond to individual requests for access to, and correction of, their personal health information
- Making your organization's privacy policies and practices available to the public
- Developing a privacy breach response protocol and ensuring everyone understands their role in the event of a breach
- Assessing and revising your privacy program on an ongoing basis

So, whether you are a sole health care practitioner who takes on this role yourself or part of a larger practice with a designated employee (or team of employees) whose full or part-time job it is to focus on this, it is crucial to assign someone these critical responsibilities for protecting personal health information.

The role and responsibilities of the privacy officer and anyone else with responsibilities related to privacy should be clearly defined in their job descriptions. Please see Appendix 1 for a sample job description of a privacy officer.

2.3 Conduct a data inventory

A good privacy management program begins with understanding the scope of the personal health information that is in your custody or control. Creating an inventory of all the personal information you hold is essential. No matter the size of your organization, it is critical to be aware of the types of personal health information your practice is accountable for and where that information is located. How sensitive is the information? Under what authority did you collect it, how is it being used or disclosed, and how long it should be retained?

After making a list of the data that you hold, you should ask yourself:

- What personal health information do I need to operate my practice?
- Why do I need it? What's the purpose?
- Do I need all of it or can I make do with less?
- Do I need to keep it, and if so, for how long?

Think carefully about the reasons for having different kinds of information and what is necessary to serve your patients. Custodians should seek legal advice and refer to the legislation, regulations, and guidelines governing members of their profession (if applicable) and any other applicable law for additional information on any record keeping requirements. You should generally not retain personal health information for any longer than is legally required, after which you must securely dispose of it in accordance with best practices for destruction (see chapter 5).

You should also consider whether de-identified information rather than personal health information can meet your purposes.

De-identification is the process of removing from a record or data set any information that identifies an individual or could reasonably be used, either alone or with other information, to identify the individual. This can be a complex and technically challenging process. If it is not done properly, there is significant risk that individuals may be re-identified. If you are considering de-identifying some of your data holdings, you should seek advice from experts in the field. You, or the expert whose advice you are seeking, should consult the IPC's in-depth **De-Identification Guidelines for Structured Data**.

Remember, the more information you collect, the more risk you assume for protecting it! You must always minimize the amount of personal health information you collect, use, retain and share with others to only what is minimally necessary.

Always put yourself in your patients' shoes and only use their information in ways they'd reasonably expect so that there are never any bad surprises.

2.4 Identify and mitigate privacy risks ahead of time

Implementing new information systems, technologies, programs, or processes or changing them in a significant way, may create risks for your patients' privacy and the security of their personal health information. As a health information custodian, you are accountable for identifying and managing these privacy and security risks ahead of time.

A privacy impact assessment (PIA) is a risk management tool that can be used to identify the potential risks associated with changes to your organization's information practices and the means necessary to proactively address them. PIAs are widely recognized as a best practice in Ontario, across Canada, and globally. They have become essential tools for anticipating and mitigating the privacy impacts associated with new or different information management systems, technologies, programs and processes.

Carrying out a PIA does not need to be complex or time consuming, but thoroughness is necessary to ensure that potential privacy and security risks are properly identified, assessed, and reasonably mitigated. The complexity of a PIA will depend on the complexity of the new information practice you are introducing or change you are considering.

The IPC has published a **PIA guide** that is intended to help organizations carry out effective assessments, as well as **Privacy Impact Assessment Guidelines for the *Ontario Personal Health Information Protection Act***, which has more specific guidance for the health sector. Smaller organizations may wish to consider engaging outside experts to help them conduct PIAs and benefit from the value of their advice and support.

2.5 Working with service providers

Most small health care organizations lack the resources needed to do everything in-house. They rely instead on service providers to support a variety of functions, such as providing and maintaining an electronic medical record (EMR) system. They may use third party vendors to provide billing or transcription services. They might subscribe to digital apps, platforms, and tools for delivering digital services like virtual care or artificial intelligence (AI) scribes. However, it's important to remember that even when functions are outsourced to third parties, it's the health information custodian who remains ultimately accountable for protecting patients' privacy and providing access to their personal health information.

PHIPA sets out specific requirements for certain types of service providers that provide custodians with electronic means to collect, use, modify, disclose, retain, or dispose of personal health

information. For example, these electronic service providers (ESPs) must not use the personal health information for anything other than what's necessary to provide the service and cannot disclose it under any circumstances. ESPs must also ensure that their employees or any other person acting on their behalf are also in compliance with these statutory restrictions.

In addition, a health information network provider (HINP) who provides information technology that allows two or more custodians to share personal health information electronically must fulfil other statutory requirements. For example, they must notify the custodian of any breach of personal health information and must provide the custodian with a threat risk assessment and privacy impact assessment of the services provided.

Whether using the services of an ESP, a HINP, or any other service provider, custodians should use written agreements setting out the roles and responsibilities of all parties involved. These written agreements should establish clear expectations detailing what each party needs to do to protect privacy in compliance with PHIPA and how compliance will be monitored. In fact, PHIPA explicitly requires written agreements between HINPs and custodians that outline the services that the HINP is required to provide for the custodian, describe the administrative, technical, and physical safeguards that will be used to secure the privacy and security of the information, and require the HINP to comply with PHIPA and its regulations. In addition, if an ESP or HINP also functions as an agent of the custodian, the requirements with respect to agents, must be complied with.

Working with third parties means entrusting someone else to play a role in protecting the privacy of your patients, so it's important to choose vendors wisely. As custodians, you should carefully vet any service provider you are considering working with to ensure they have the necessary capacity and a good track record for complying with all applicable PHIPA requirements. In some cases, you can look for programs that are offered by trusted health sector stakeholders to help assess solution providers: such as OntarioMD's certification program for **Electronic Medical Records (EMRs)** or Ontario Health's verified solutions list for **virtual visits** available at **www.ontariohealth.ca**.

You can also refer to the IPC's guide to **Privacy and Access in Public Sector Contracting with Third Party Service Providers**, which includes practical advice and best practices for ensuring proper accountability when considering working with third party service providers and building in privacy and security considerations throughout the procurement process from beginning to end.

Quick Tips!

- Evaluate potential service providers to determine that they both understand and can meet defined privacy, security and all other requirements.
- Ensure that any arrangements with service providers address privacy, security and all compliance requirements with clear terms and conditions.
- Clearly establish the roles and responsibilities of all parties to a contract or agreement, from beginning to end.

2.6 Set your team up for success

Working effectively with your team to ensure PHIPA compliance is an important part of your clinical practice. It's also a key building block of your privacy management program. Good communication and training will support the people working for you and help promote and foster a culture of privacy throughout your organization.

Did you know?

The actions of employees, through human error or negligence, are the largest cause of security breaches.

Good habits should be instilled from the start. This begins with your employee onboarding practices. Any staff member who works with personal health information must clearly understand their role as a PHIPA agent and their specific responsibilities regarding that information, including physicians. Training materials should be updated with any new legal requirements, lessons learned, or any time there is a significant change to your information practices. Training is an ongoing responsibility: it should be delivered on a regular basis, and tracked to ensure all staff have successfully completed it.

For a practical understanding of why this matters, see lessons learned and other key takeaways in the IPC's case note Preventing health privacy breaches: why training, policies, and confidentiality agreements matter.

All staff should be trained on your policies, procedures and controls so they know how to keep personal health information private and secure, and how to identify and report potential breaches. This is true even for employees who do not work directly with personal health information. For example, even though an employee does not normally interact with personal health information as part of their job, they may receive personal health information by mistake, may be the subject of a phishing attempt, or may suspect a cybersecurity incident. All employees, therefore, whether they are agents or not, must know what they need to do in such cases. Training should be reinforced with ongoing communication to maintain a high level of privacy awareness among staff.

Quick Tips!

- All staff must receive privacy training before starting their employment or contractual relationship and before being granted access to personal health information.
- Ongoing refresher privacy training should be provided on a regular basis or when changes in policy, regulations, or legislation occur.
- Training should test your staff's understanding of Ontario's privacy requirements.
- Role-based privacy training is a useful method to help to ensure people understand how to apply privacy policies and procedures in their day-to-day work.
- Mock scenarios, like privacy breach simulations, could help everyone practice how to respond when a real breach happens.
- Privacy training materials should be reviewed and updated on a regular basis.
- Successful completion of required training by each employee should be tracked for good record-keeping practices.

2.7 Get everyone's commitment

To ensure your team members acknowledge their privacy obligations and commitments, you should have written confidentiality agreements in place with each of them that set out their privacy obligations and commitments and explain the consequences of a privacy breach. Privacy should be top of mind for all employees, whether or not they act as your agents in their day-to-day job duties.

Confidentiality agreements should be signed at the start of employment (or other arrangement) and re-signed on an annual basis. Be sure to keep a record of who signed the agreement and keep track of it, so it stays up to date.

Confidentiality agreements with employees should:

- Require all employees to acknowledge that they have read, understood, and agree to comply with your privacy policies and procedures, and attest that they understand the potential consequences of non-compliance.
- In the case of agents more specifically, define the purposes for which agents are permitted to collect, use, and disclose personal health information, including any limitations, conditions or restrictions, and confirm that they understand their role and responsibility to comply with PHIPA and its regulations.
- Require all employees to securely return all property at the end of their contract or employment, including a requirement for agents to return any personal health information they may have.
- Specify that you may conduct random privacy and security audits to periodically check compliance with privacy and security policies and procedures.
- Require employees to notify you of any privacy or security breach at the first reasonable opportunity.

2.8 Be clear about the consequences of non-compliance

Part of a robust governance and accountability framework is making clear what will happen in the event of non-compliance. Custodians should outline the consequences if an employee or agent violates privacy policies or procedures or otherwise fails to meet their privacy-related obligations.

Adopting a just culture approach means taking a proportionate approach in response to privacy violations. Honest mistakes can be used as a learning opportunity to remind and retrain staff on how to avoid repeating them in the future. Depending on their frequency and severity, some errors may invite more serious corrective measures and/or disciplinary action, up to and including suspension or even termination. In yet more egregious cases, privacy violations may result in administrative monetary penalties imposed by the IPC or be prosecuted by the Ministry of the Attorney General as an offence under PHIPA. These consequences can be imposed on the accountable custodian, as well as the individual(s) responsible for contravening PHIPA.

It's important to be clear with employees about the following matters:

- Describe the types of privacy violations that may invite corrective measures or disciplinary action.
- Outline possible consequences of breach and the factors that will be considered in determining the appropriate corrective or disciplinary action to be taken, including escalation measures and possible involvement of relevant professional regulatory bodies.
- Explain how some cases of non-compliance may be the subject of an investigation, and who will be responsible for performing the investigation and reporting the results.
- Describe any documentation that will be completed, provided, and/or executed in the context of an investigation and how long the results will be retained on file.
- Explain that in some cases, the IPC may investigate cases of non-compliance that may result in public reports, legal orders to stop or change certain information practices, and possibly administrative monetary penalties.
- In the most egregious cases, non-compliance may even be prosecuted by the Ministry of the Attorney General as an offence under PHIPA, resulting in steep fines or even imprisonment.

There can be serious consequences for failing to protect privacy. Where a person is found guilty of an offence under PHIPA, this may result in fines of up to $200,000 for individuals or to a term of imprisonment of up to one year or both, and $1,000,000 for organizations. As of 2024, the IPC also has the power to issue administrative monetary penalties (AMPs) as part of its broader enforcement powers for violations of PHIPA or its regulations. These penalties may reach a maximum of $50,000 for individuals and $500,000 for organizations. The IPC may increase the penalty by an amount equal to the economic benefit gained by the person who contravened PHIPA. For more information about AMPs and the IPC's approach to enforcement, please refer to the guidance document **Administrative Monetary Penalties: Guidance for the Health Care Sector**. Or you could watch a short educational IPC FYI video, available on the IPC's YouTube channel called **A Guide to AMPS** that explains it in briefer, simpler terms.

2.9 Have a back-up plan in place

Maintaining control of the information that you're responsible for is an important part of accountability. Computer systems can be hit by power outages, thieves, or cyberattacks, which may result in theft, loss, and unauthorized use or disclosure of personal health information. It is considered good practice to have a business continuity and disaster recovery plan in place to ensure the continued availability of your information environment in the event of short and long-term business interruptions. At minimum, the plan should include:

- A description of your back-up methods, and how back-ups will be used in the event of short or long-term business interruptions.

- Procedures for the secure and timely restoration of files and systems from backups and system images, and the routine testing of such procedures.
- Policies addressing how often records of personal health information are backed up (e.g., daily, weekly, etc.) and where they will be securely stored.

Custodians should seek guidance from their service provider for more information on their system's backup and recovery capabilities and the available options for off-site backup. Your agreement with the service provider should address the security of backups and set out clear retention policies.

Having an off-line back up is a good way of protecting your organization and your patients' personal health information from the paralyzing effects of a cyberattack. Read about this and other key takeaways from the IPC's case note Ransomware reality: Case study in health care cybersecurity and recovery.

RECAP! Governance and accountability: Key steps to take

- **Set a privacy respectful tone:** Foster a culture that embodies foundational privacy principles.
- **Assign clear roles and responsibilities:** Designate a privacy officer to develop and run your privacy program.
- **Conduct a data inventory:** Understand the scope of the information that is in your custody or control and minimize the collection to only what is necessary.
- **Consider the need for PIAs:** A systematic approach to assessing new, or changes to, information management systems, programs, or technologies can help identify and mitigate privacy risks.
- **Choose vendors carefully**: Address privacy and security considerations when considering working with third party service providers, such as EMR providers, and build these into your contractual arrangements.
- **Train and communicate:** Ensure you and any staff have the proper privacy knowledge and skills on an ongoing basis, and make sure to regularly update your training materials as needed.
- **Get commitments:** Staff should sign confidentiality agreements on an annual basis attesting that they understand and commit to following privacy policies.
- **Be clear about consequences:** Make sure that staff understand what will happen if policies aren't followed, ranging from learning opportunities and retraining, to possible disciplinary action and legal consequences.
- **Prepare for disaster:** Make disaster recovery plans and prepare how you will resume operations in the event of significant business interruptions.

3.0 Develop and document your privacy policies

Your privacy management program is driven by the values and commitments that underlie your information management practices. Some of these values and commitments will be driven by the requirements set out in PHIPA, while others may go beyond strict legal requirements, and reflect a privacy–first culture.

3.1 Define your privacy commitments

As part of your privacy management program, you need to develop written policies and procedures that embody those values and commitments.

Policies vs procedures?

It's important to know the difference between a policy and a procedure. It's easy to confuse these two, but they have very distinct purposes and uses.

- **A policy** describes the what and why. It has a broad application.
- **A procedure** describes how you are implementing the policy.

Policies are for both internal and external use, while procedures are typically for employees only. In this chapter, we will discuss what to include in your policies. In chapter 5, we will discuss the types of procedures you need to put in place to operationalize your policies.

3.2 Document your privacy policies

Policies form the backbone of every privacy management program. Policies are an essential foundation for handling personal health information effectively and being explicit — both internally and externally — about your commitment to do so.

What is a policy?

A policy is a written document that sets out your privacy commitments and the standards by which you manage information. Policies come in all shapes and sizes. They define the rules that must be followed by anyone — e.g., agents and contractors —who interacts with the personal health information under the control or custody of your practice.

Do you need privacy policies?

Absolutely! Formalizing policies in writing makes good legal and business sense. Clear and well-written policies will guide you, your team, and anyone else who may handle personal health information under your stewardship so that everyone knows what they can and cannot do with the information, and how to protect it. Maintaining privacy policies also helps build trust with your patients and makes them feel more secure. It shows your commitment to treating their personal health information with the utmost care.

Where to start?

The policies you create should be tailored to the size and business model of your practice and the kind of data you collect. Some health care providers have separate documents detailing different privacy-related policies, while others have an overarching privacy policy that integrates many policies into one document.

As a small health care operator, it may be easier to have all your privacy-related policies in one document.

The chart below summarizes the basic information you need to include in your privacy policy or policies. Remember, some elements may not apply to all health practitioners; your policy will depend on the size and scope of your practice. In the appendix, we provide a sample template you can use to address more detailed program components that must be included in your privacy policies.

Your privacy policy: What should it cover?	
Purpose: **Why do you need the patient's personal health information?**	• Outline your commitment to respecting patient privacy. • This can include your obligations as a custodian to comply with PHIPA and its regulations. • Describe why you need the patient's personal health information and what you plan to do with it.
Collection: **How will you collect the information?**	• State all the ways you will collect personal health information from patients (e.g., print forms, digital apps, from other health care providers, etc.) • Describe the sources from which you collect information about patients (e.g., medical laboratories, imaging clinics, pharmacies, other healthcare providers, and in some cases, substitute decision-makers)
Use: **How will you use the information?**	• Identify the different purposes for which you may use the information. Primarily, this will be for purposes of providing health care. • However, it might also include other purposes, such as for error or risk management, to improve or maintain the quality of health care services. Or it may be the purpose of billing, processing claims and obtaining payment for the health care you provide your patients.

Your privacy policy: What should it cover?	
Sharing: **How will you share the information with others, if at all?**	• Describe how and when you may share (disclose) the information, and with whom, provided you meet the conditions under PHIPA. • For example, this might include other health care providers or specialists for the purpose of providing care, the Ministry of Health for the purposes of billing, outside researchers for the purpose of conducting a research study, or public health officials to improve health at the population level.
Protection: **How will you protect the information?**	• Identify how and where the information will be stored. • List the physical, technical, and administrative security safeguards you'll use to protect personal health information. • Describe how long you'll keep the information for, and how it will be permanently and securely destroyed once no longer needed.
Responding: **How will you respond to patient privacy inquiries, as well as potential breaches of information?**	• Describe your process for handling privacy concerns, complaints and requests from patients. Remember, patients are entitled to request a copy of their health records and can request corrections and updates to their personal health information. • Identify the person/position to whom patient inquiries or complaints may be directed, including their contact details. • Describe how you'll handle a privacy incident or breach (i.e., if personal health information is lost, stolen, or used or disclosed without authorization), including notification to any affected individuals and where necessary, the IPC. • Be clear about a person's right to complain to the IPC and identify the process for doing so.

Your privacy policy: What should it cover?	
Consent: **What form of permission do you have to collect, use, and share personal health information?**	• Specifically identify the circumstances in which your practice relies upon express, or implied consent for the collection, use, and disclosure of personal health information. • For example, personal health information can only be disclosed to a custodian for purposes other than providing health care, or to a person that is not a custodian with the patient's express consent. This would include disclosures to a patient's lawyer or insurer, for example. • Express consent is also required for any collection, use, or disclosure of personal health information for the purposes of marketing or market research. However, the PHIPA regulation excludes communication with patients from practitioners who provide insured services about additional uninsured services that may be provided on a fee-for-service or through a set annual fee from the definition of marketing. • Custodians may rely on implied consent to collect, use, and disclose a patient's mailing address, and/or the name and mailing address of a substitute decision-maker for fundraising purposes. However, any collection, use, or disclosure of other forms of contact information (such as a phone number or email address), or of other information about the patient's health condition or their receipt of health care for fundraising purposes requires express consent. Note that the PHIPA regulation prescribes additional important requirements and restrictions that apply to all collections, uses, and disclosures of personal health information for fundraising. Please refer to the IPC's fact sheet **Fundraising under PHIPA** for additional details. • Otherwise, most health care providers, may rely on a patient's implied consent to collect, use, or disclose their personal health information for the purposes of providing them with health care or referring them to other health practitioners for diagnostic tests or specialized treatment, where certain conditions are met. For more information about sharing information for health care purposes, refer to the IPC's guidance: **Circle of Care: Sharing Personal Health Information for Health-Care Purposes**. • Patients have the right to withhold consent or restrict who gets to access their record. Know that patients' consent directives are subject to exceptions, such as where the disclosure is for the purpose of eliminating or reducing a significant risk of serious bodily harm. For more information, refer to the IPC's **Lock-box Fact Sheet**.

Your privacy policy: What should it cover?	
Consent: **What form of permission do you have to collect, use, and share personal health information? (Cont'd)**	• Be clear about circumstances where the collection, use, or disclosure of a patient's personal health information may be permitted or required by law without their consent, such as for billing purposes, health planning, evaluation or research, subject to applicable conditions. • Explain situations in which patients may rely on substitute decision makers to make decisions on their behalf, such as for minors or adults who lack the capacity to give consent on their own. There are specific requirements with respect to who may act as a substitute decision maker and under what circumstances. Please refer to the IPC's **A Guide to the *Personal Health Information Protection Act*** for additional information about capacity and substitute decision-making.
Monitoring: **How will you monitor and enforce compliance with the policy?**	• Outline the actions you will take to ensure employees and others follow the policy. • Explain how you will monitor compliance and periodically conduct privacy and security audits. • Be clear about the consequences of non-compliance. • Mention that the policy will be periodically updated to reflect necessary changes arising from recommendations resulting from privacy impact assessments or privacy and security audits, changes to legal or regulatory requirements, and/or evolving best practices.

3.3 Tell patients and other stakeholders

Once you have developed and documented your internal privacy policies, you're ready to inform patients and others about your information practices. Under PHIPA, practitioners are required to have a written public statement available that provides a general description of how you protect and handle personal health information.

Your internal privacy policies may be suitable to share externally as they are. In other cases, they may need to be modified for easier readability for people outside your practice. Whatever the case, you must have written information publicly available and readily accessible that:

- summarizes your information practices
- provides contact information for a designated point person in your organization
- describes how individuals may make a request to access or correct their personal health information
- explains how an individual can make a privacy complaint with you and/or the IPC if they have concerns with your compliance with PHIPA

You can choose an appropriate name for your written public statement, such as privacy notice, external privacy policy or information practice statement. For simplicity here, we'll refer to it as a privacy notice.

Preparing your privacy notice: Quick tips for success

Have you ever read a privacy notice for an app or website before clicking to accept the terms? Probably not. But you're not alone. Research shows many people never read a privacy notice before agreeing to it. Why? Because they tend to be too long and confusing, written to satisfy legal compliance requirements and regulators instead of being truly useful for the purpose of informing individuals.

Here are tips to ensure your privacy notice explains your information practices effectively — and will be understood by your patients and others:

- **Clear language:** Aim to write a patient-friendly notice that's easy for people to understand. Avoid using technical or legal jargon.
- **Be transparent:** Be open about how you use, or plan to use, people's personal health information. They have a right to know. You should give a copy of your privacy notice to patients when you first collect their personal information.
- **Contact details:** Let people know who to contact within your practice if they have questions or concerns about your privacy practices. Under PHIPA, you must also provide information on how to reach the Office of the Information and Privacy Commissioner of Ontario if they want to file a complaint.
- **Keep it concise:** If it's short and simple, it's more likely to be read. You don't have to tell people everything in detail. Summarize the essential points.
- **Layered approach:** Provide the information in digestible chunks, using short paragraphs, clear headings, and bulleted lists, offering to provide more details on request.
- **Visual presentation:** Consider using graphics, images, icons, and other visual aids to make the information more engaging and easier to understand for diverse audiences.
- **Accessible:** Make sure your privacy notice is readily available and easy to access if people want to read it now or later. For example, it can go on a poster or in a pamphlet at your clinic, with a link or QR code that sends patients to your website for more detail.

RECAP! Commitments and policies: Key steps to take

- Define your privacy commitments.
- Write your internal privacy policies that document:
  - The purposes for collection, use, and disclosure of personal health information
  - The ways in which you will collect information
  - The ways that your practice uses personal health information
  - How personal health information may be shared
  - The general ways that you protect personal health information
  - How you will respond to patient privacy inquiries, as well as potential breaches of information
  - Consent requirements for collecting, using, and disclosing personal health information
  - How you will monitor and enforce compliance with the policy
- Create an external-facing public statement for patients and other stakeholders that:
  - uses clear language
  - is transparent
  - provides contact details
  - is clear and concise
  - uses a layered approach
  - is visually engaging and meaningful
  - is readily accessible

DEVELOPING YOUR PRIVACY PROGRAM

4.0 Safeguarding personal health information

The relationship between individuals and their health care providers is based on trust. Individuals provide intimate details about their health and wellness, in confidence, to their health care providers to receive the best care and treatment.

People share their personal health information with their health care provider with the expectation that it will be protected. If patients' expectations of privacy and confidentiality are not met, their trust may be irreparably damaged. This may have serious repercussions for individuals, health care providers, and the entire health sector.

Unfortunately, privacy breaches sometimes happen. This might involve situations where, for example, custodians or their agents access records without authorization, or where they use or disclose personal health information for purposes for which they are not allowed. Unauthorized access, use, or disclosure may be the result of carelessness or inadvertence, or it may be motivated by an intention to snoop into records of family members, neighbors, or famous people. Sometimes, it may be done out of sheer curiosity or a misplaced concern about the health and well-being of individuals when there is in fact no real need to know such information. Other times, it may done deliberately to cause embarrassment or harm to others, or for personal economic gain.

Other times, privacy breaches are caused by external threat actors, like cybercriminals, who gain unauthorized access to your information systems. They might threaten to expose your patients' personal health information on the dark web unless you pay them a ransom, or they may lock down your information system to paralyze delivery of your services until you pay up. Either way, such cyberattacks can be devastating to you, your practice and the trust of your patients.

PHIPA requires that, as a health information custodian, you must take reasonable steps in the circumstances to ensure that personal health information in your custody or control is protected against theft, loss, and any unauthorized use, disclosure, copying, modification, or disposal.

This chapter highlights some important safeguards and considerations for protecting personal health information under your care. Because best practices for information security are constantly evolving, we recommend you consult additional resources and seek expert advice when developing your security policies and procedures.

Develop strong security controls

As custodians, you are accountable for personal health information in your custody or control and for the actions of your agents with respect to that information. Your obligation to safeguard personal health information arises regardless of its form (oral, paper or digital), wherever it is kept (office, home, online, a third party, etc.) and however it may be transferred (via email, voicemail, mail, etc.)

PHIPA requires that you implement reasonable technical, physical, and administrative security safeguards to protect personal health information against theft, loss, and any unauthorized use, disclosure copying, modification, or disposal.

Therefore, to fulfil your safeguarding obligation, you must take steps that are reasonable in the circumstances to protect personal health information from potential privacy and security risks. It's important to take a multifaceted approach to detecting, preventing, and reducing such risks, including by implementing:

Technical safeguards

- use only organization-approved email, messaging, or videoconferencing accounts, software, and related equipment
- use firewalls and protections against software threats
- regularly update software applications with the latest security and anti-virus software
- encrypt data on all mobile and portable storage devices, both in transit and at rest
- maintain, monitor, and review audit logs
- use and maintain strong passwords
- review and set default settings to the most privacy protective setting
- verify and authenticate a patient's identity before engaging in an email exchange, chat, or videoconference
- conduct regular threat risk assessments

Physical safeguards

- keep all technology containing personal health information, such as desktop computers, in a secure location
- when unattended, keep portable devices containing personal health information, such as smartphones, tablets, and laptops, in a secure location, such as a locked room, drawer or cabinet
- restrict office access, use alarm systems, and lock rooms to protect equipment that is used to send, receive, or store personal health information
- do not lend technology containing personal health information to anyone without authorization
- ensure there are no unauthorized persons in attendance or within hearing or viewing distance when conversing with patients
- physically segregate and restrict access to servers to only authorized persons

Administrative safeguards

- ensure employees are aware of the prohibition against collecting, using, or disclosing personal health information without authorization
- ensure employees are properly trained to use secure email, messaging, and videoconferencing platforms and ensure ongoing security training to support the detection of phishing attempts
- adopt a robust system of access controls and regularly maintain authorizations on a need-to-know basis
- ensure confidentiality agreements contain explicit provisions dealing with employees' obligations when using secure email, messaging, or videoconferencing and renew these on an annual basis

Safeguarding against privacy security risks is an ongoing obligation. You must take reasonable steps to proactively monitor for and address new cybersecurity threats, and continually adapt your technical, physical, and administrative safeguards accordingly.

Avoid use of faxes

For a long time, health providers have communicated with one another by fax. This mode of communication has become antiquated, and relatively insecure. In fact, a large proportion of privacy breaches reported to the IPC are the result of misdirected faxes — faxes that were sent to the wrong number or the wrong person, resulting in breaches of patient confidentiality.

The IPC has long advocated to reduce, and even eliminate, the use of faxes in Ontario's health sector. As part of the government's pledge to "**help family doctors put patients before paperwork**," it promised to "axe the fax" by replacing fax machines with other digital communication devices by 2028 "to speed up diagnosis, referrals and treatments while improving the privacy of patient's health information." We strongly encourage you, as health providers, to transition to more secure forms of digital communication.

For an example of an institution that suffered from large numbers of misdirected faxes and put in place successful measures to help reduce its reliance on faxes and mitigate the risk of breaches, see the IPC's report on St. Joseph's Healthcare Hamilton.

Additional safeguards for email and secure messaging applications

While email communications and other digital messaging applications offer many benefits as part of a modern health practice, they also pose risks to the privacy and confidentiality of patients. As custodians, it is important that you understand these risks and take reasonable steps to mitigate them before using these tools for professional communications. The IPC's fact sheet, **Communicating Personal Health Information by Email** outlines many of the factors you should consider when determining whether to use such tools, and how to meet your obligations under PHIPA when doing so.

If you decide to use email and other digital messaging apps, you should address this in your privacy policy. Specifically, your policy should address when, how, and for which purposes personal health information may be sent and received via messaging applications, as well as any conditions or restrictions on doing so. The policy should also set out what types of information should only be sent and received using encryption and the circumstances in which unencrypted communications may be acceptable.

One of the unique challenges for using digital tools to communicate directly with patients — particularly when you cannot see or hear the patient — is to ensure the exchange is with the correct person. It's important to take steps to verify the recipient's identity and correctly address messages to avoid misdirection. One approach is to send a test message in advance and ask for confirmation to ensure the message reaches the intended recipient. Further safeguards to use when communicating personal health information via email include:

- providing a notice in an email that the information received is confidential
- checking (and rechecking again!) whether the appropriate individuals are included in the "to" and "cc" boxes
- providing instructions to follow if an email is received in error
- communicating by email only from an approved professional account
- confirming an email address is up-to-date
- ensuring that the recipient's email address corresponds to the intended address
- regularly checking pre-programmed email addresses to ensure that they are still correct
- restricting access to the email system and to email content on a need-to-know basis
- acknowledging receipt of emails
- minimizing the disclosure of personal health information in subject lines and bodies of emails
- ensuring strong access controls to email accounts
- recommending that patients use a password-protected email address that only they can access

Encryption

Email communications between custodians that contain personal health information should be secured from unauthorized access through encryption. When communicating with patients, you should also use encryption especially when relaying personal health information. This includes encrypting or password-protecting document attachments and sharing passwords separately through a different channel (for example, if encrypted documents are sent using email, the password could be sent by text message). If the use of encryption is not feasible, you must determine if the use of unencrypted email is reasonable in the circumstances after considering all relevant factors, including the sensitivity of the information, the purpose of the transmission, and the urgency of the situation.

Storage

Moreover, personal health information should only be stored on email servers for as long as is necessary to serve the intended purpose. For example, if email communication is documented in the patient's records of personal health information, it may not be necessary to retain duplicate copies of the information on an email server. Likewise, you should ensure that all copies of emails containing personal health information on portable devices are securely deleted as soon as they have been documented in the patient's record, and they are no longer needed.

For best practices on using email and other digital messaging apps, please see the IPC's fact sheet: **Communicating Personal Health Information by Email**.

Phishing

Phishing is an online attack in which an attacker — using both technological and psychological tactics — sends a message designed to trick the recipient into revealing confidential information or downloading malware. Phishing attacks often imitate legitimate sources and work by exploiting people's trust, curiosity, fear, or desire to be helpful and efficient. Your employees must be regularly trained to detect, avoid, and report phishing attempts. Even your patients should be informed how to recognize the risks associated with phishing to avoid falling prey to malware, spyware, or other forms of social engineering.

Recipients should be cautious when faced with messages that are unexpected or contain suspicious attachments or links. For example, phishing emails that appear to be sent at odd hours, containing typos or strange user and domain names, requiring urgent action under the pretext of some emergency should trigger l alarm bells. Ask your employees and your patients to alert you immediately in such cases, and to avoid responding to such emails, clicking on any suspicious links, or opening any attachments.

For best practices and practical tips, please see the IPC's fact sheet Protect against phishing. Or, listen to the *Info Matters* podcast episode, Don't get caught! Protect yourself against phishing.

Additional safeguards for videoconferencing

Virtual health care services have proven to be very practical and beneficial when serving remote populations, or during times of public health emergencies, like the COVID-19 pandemic. However, virtual health services also raise unique privacy and security concerns because of the novel technologies and communication infrastructures they use, and the online environments in which they operate. Just as with other digital tools, it is important for custodians to understand these risks and take steps to mitigate them before adopting virtual care technologies.

When using videoconferencing platforms to deliver care, it's important to take additional steps to protect patient privacy:

- As a best practice, both you and your patient should join the videoconference from a private location using a secure internet connection. This includes using a closed, soundproof

room or an otherwise quiet and private place and having window coverings where and as appropriate. Use headphones rather than the speaker on the device to prevent being overheard by others and be mindful of where screens are positioned.

- Once logged into the videoconference, you should check the meeting settings to ensure the meeting is secure from unauthorized participants. If the software or application can record the meeting, this feature should only be used when it is necessary and if the patient provides express consent.
- At the start of an initial visit, it's important to verify the identity of the patient. In the event of a new patient encounter, you should compare the patient's image with a photo on file or ask the patient to hold up their health card to the camera for confirmation.
- Be sure to introduce yourself and any others who are present on the custodian side of the interaction and ensure the patient consents to the presence of any additional individuals. You should also inquire if anyone is accompanying the patient and confirm the consent of the patient.
- It's important to use sufficiently high-quality sound and resolution to ensure that you are able to collect information (including verbal and non-verbal cues) that is as accurate and complete as is necessary for the purpose of providing health care.

For additional information about managing privacy and security risks associated with virtual care tools and technologies, please see the IPC's guidance document: Privacy and security considerations for virtual health care visits.

Additional safeguards for the use of artificial intelligence (AI)

Ontario's health sector has recently seen substantial growth in the use of artificial intelligence (AI) technologies aimed at assisting health care providers with their administrative responsibilities. The most popular of these are referred to as AI scribes. Depending on the features of a specific product, an AI scribe may be able to transcribe or summarize health care visits, populate personal health information into EMRs or EHRs, and produce medical notes or reports. Many AI scribes are evolving to offer additional features such as initiating referrals, ordering medical tests, and even recommending diagnoses and treatments.

While AI scribes have the potential to lessen the administrative burdens of health care providers in Ontario, it is important to consider the potential challenges that arise specific to AI technologies. The following are examples of some of the additional steps you should consider taking to protect patient privacy when procuring, implementing, and using AI scribes.

- First, you are responsible for ensuring that your have the legal authority to collect, use, and disclose personal health information. In the context of AI scribes, this means carrying out the necessary due diligence to ensure that the underlying data used to develop and train the AI scribe's model was, and continues to be, obtained lawfully.

- Furthermore, you must ensure that you have obtained patient consent before using an AI scribe and that you are very transparent with your patients about the purposes, risks, and implications of doing so.
- You must take reasonable steps to ensure that the AI scribe has been developed and is maintained in a secure and privacy protective manner. One way to do this is by conducting a privacy impact assessment (PIA), threat risk assessment (TRA) where appropriate, as well as an AI specific assessment, known as an Algorithmic Impact Assessment (AIA). These assessments are not a one-and-done exercise and should be regularly updated, especially before deploying any new use or added feature of an AI scribe.
- An AI scribe is a generative AI technology that changes over time as it continues to learn from new data — therefore you should ensure that the AI scribe's model is continuously monitored and evaluated for validity, reliability, and accuracy throughout its use to ensure the ongoing safety to your patients.
- You must ensure that you have strong contractual safeguards in place with the AI scribe vendor to protect patient privacy. This includes carefully reviewing the terms of service of the vendor to ensure that the vendor does not use patient information for any purposes other than providing the service and that the vendor commits to meeting their obligations under PHIPA.

As small health providers, you may not have the necessary capacity or resources to do all of this yourself. You may want to seek outside experts to help you navigate these issues.

For further information, please refer to the IPC's guidance: Procuring, Implementing, and Using AI Scribes: Key Considerations for the Health Sector. You may also wish to listen to the IPC's *Info Matters* podcast episode, Artificial Intelligence in health care: Balancing innovation with privacy.

Logging, auditing, and monitoring

The logging, auditing, and monitoring of all accesses to electronic records of personal health information is important to ensure the privacy of individuals and the confidentiality of their personal health information. Logging all instances where personal health information is collected, used, and disclosed will enable you to audit and monitor your agents' activities, respond to any privacy complaints received and investigate actual or suspected privacy breaches including cases of unauthorized access.

Key terms

Logging: the process of recording events in computer systems and networks. Logging captures data from various sources and monitors system and network activities to protect against and identify unauthorized access, use, or disclosure.

Auditing: refers to the review and examination of logs, other records and activities to review compliance with policies and procedures and evaluate the adequacy of privacy and security controls.

Monitoring: ongoing, often automated observation of data collected from computer systems and networks to identify unusual patterns and anomalies that may be indications of attacks or unauthorized activities.

Logging, auditing, and monitoring can also be an effective deterrent to unauthorized access if your agents know that their access to and use of digital systems will be logged, audited, and monitored on an ongoing, targeted, and random basis. In general, you should ensure that information systems containing personal health information can log all instances where the information is collected, used, or disclosed, as well as all instances where there is an override of a patient's consent directive or the by-passing of a privacy warning flag. By referring to the logs, you should be able to determine, at a minimum:

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

Ideally, logs will also indicate the duration of access to a record.

Some third party audit tools can systematically and automatically analyze access logs and generate reports based on defined search criteria. By automating manual processes using a variety of queries, these third party tools can help ensure greater efficiency in audit reviews and help prevent and detect unauthorized access to personal health information. For instance, they can help identify usage patterns of agents' access in electronic information systems consistent with certain types of misbehaviour or irregular activity. By automatically generate alerts or reports, they could help raise early flags, warning you of potential problems and trigger the need for further auditing.

For more detailed information, please refer to the IPC's guidance document: Detecting and Deterring Unauthorized Access to Personal Health Information.

RECAP! Safeguarding personal health information

- **Implement and regularly review reasonable technical, physical, and administrative security safeguards** to protect the personal health information in your custody or control.
- **Avoid the use of faxes**. Misdirected faxes are a significant source of privacy breaches.
- **If using email or other messaging applications** to communicate with other providers and your patients, be sure to use encryption, securely transfer communications into the patient's record, and delete messages from servers or portable devices when no longer required.
- Train your employees to detect, avoid, and report **phishing attacks**, and inform your patients of risks of phishing attacks as well.
- Follow best practices to protect privacy and confidentiality when using **videoconferencing** for virtual visits.
- If considering using **AI scribes**, give careful consideration to potential risks and harms, and take active steps to mitigate them from the start.
- **Ensure that logging is enabled** for all digital systems that are used to collect, use, or disclose personal health information.
- **Regularly review and audit system logs** to help detect unauthorised access and take early action to look further into any potential irregularities.

5.0 Procedures and controls: Making it operational

Now that you have developed and documented your policies, it's time to put them into practice! Making your privacy policies operational involves bringing them to life by creating procedures and controls for how you and your team will manage, use, share, and protect the information you collect.

Remember, a procedure is the detailed process for implementing a policy. While creating policies is a foundational step in establishing your privacy management framework, your procedures reflect the concrete actions you will take to meet your privacy responsibilities.

Get employees to confirm that they understand and will uphold your privacy policies

It's not enough for your employees to speed read through your privacy policies. Your employees should take (and be given) the time to carefully review your privacy policies and attest to understanding them. They need to know your data protection commitments, rules, and expectations, along with their responsibilities. It's important that they confirm they have read, understand, and will comply with your privacy policies, and that this confirmation is documented in writing.

Make sure employees successfully complete privacy training on a regular basis

Similarly, it's not enough for employees to merely go through the motions of annual privacy training. You must be able to confirm and document that they have successfully completed the required training and that they are able to operationalize your policies in practice. The use of a post-training test or quiz to confirm that employees have internalized and understood the rules they are obligated to follow can assist in accomplishing this. In addition, where any agent fails to complete any required training, ensure there is a process to follow up on this, including suspension of access to PHI where appropriate.

Review access controls on a regular basis

Identify which members of your team need to access patients' personal health information and for which purposes. Then establish responsibilities and procedures to operationalize access privileges on a need-to-know basis. Establishing role-based access ensures that your agents who deal with personal health information are only able to access the information they need to carry out their role, and no more than what is minimally required to do so. Have reminders in place to review your agents' access controls on a regular basis to ensure they remain relevant and necessary and immediately revoke access privileges of anyone who leaves the organization — whether temporarily or permanently.

Establish good record keeping practices

Good information management practices rely on good record keeping. This helps you run a smoother practice by ensuring you can find information you need more easily and in an organized way. It also provides evidence that you're taking the management of personal health information seriously and that you're taking the necessary steps to comply with PHIPA.

Be sure to document or log information you may need to track and reference in the future, such as:

- patient consent forms
- agreements or contracts with service providers
- confidentiality agreements of employees
- data sharing agreements with third parties
- research agreements with researchers
- employee attestations confirming that they have read and understood your organization's privacy policy (or policies) and have completed the required privacy training
- role-based access rights granted to agents on a need-to-know basis
- requests for access to, or correction of, personal health information and the outcomes of each request
- results of privacy impact assessments, threat risk assessments, and where applicable, algorithmic impact assessments
- privacy inquiries and complaints
- privacy breach reports
- certificates of destruction

Create record retention and destruction procedures

PHIPA requires custodians to ensure that any records of personal health information in their custody or under their control are retained, transferred and disposed of in a secure manner and in accordance with PHIPA. Keeping personal health information longer than necessary increases the risk of privacy breaches.

Here are some key things to consider:

- **Create record retention schedules:** Develop rules around record retention. PHIPA requires records of personal health information to be kept for as long as needed to allow an individual to exhaust any legal recourse regarding an access request. As PHIPA does not establish specific retention periods for personal health information, custodians should refer to their governing legislation, professional guidelines and any other applicable law to determine applicable record retention requirements.
- **Establish rationale and exceptions:** If you determine it's in the best interest of your practice and/or your patients to retain records of personal health information for longer, be sure to document your authority and your rationale to retain the information.

- **Have a secure destruction plan in place:** Once the retention timeline has expired, it is crucial to securely destroy the records in a way that ensures the record cannot be reconstructed in any way.
- For instance, **paper records** should be incinerated, pulverized or at minimum, shredded using a cross-cut shredder. Hand ripping records and disposing of them in an unsecured bin is not sufficient.

Read about practical lessons learned and key takeaways in the IPC's case note Ensuring secure disposal of health records: Out of sight is not out of mind!

- As for **digital records**, these should be permanently destroyed or irreversibly deleted or erased. Simply deleting files or formatting electronic devices is not sufficient to ensure secure destruction. To securely destroy personal health information in digital form, you must perform certain operations on the media where the information is stored. This includes, physically destroying the storage media by using special tools or services to pulverize, shred, incinerate, or magnetically degauss devices, drives or disks, or using specialized and device-specific software tools to securely overwrite stored data.
- See the IPC's fact sheets: **Secure destruction of personal information** and **Disposing of your electronic media** for more information.

Have a clear breach response protocol

Unfortunately, privacy breaches are increasingly common, particularly in the health care sector. While cyberattacks are on the rise and a major cause of breaches, a breach may also be the result of any number of actions — such as misdirecting an email or sending a bulk email about your practice without hiding the recipient addresses or sending a medical result to the wrong patient. A breach is really any case where personal data you're responsible for is somehow lost, or accidentally destroyed, damaged, or shared with someone it shouldn't have been.

A breach can have minor or serious privacy implications. As a custodian, you must take immediate action upon learning of a privacy breach. It is therefore essential that you develop and implement a comprehensive breach response protocol that outlines the steps involved in managing a privacy breach depending on its significance and risk of harm. The following steps may need to be carried out simultaneously and in quick succession in the event of a privacy breach.

Step 1: Notify staff and other custodians

- Notify all relevant staff of the breach, including your privacy officer or PHIPA contact person.
- Depending on the nature or seriousness of the privacy breach and the size and structure of your organization, you may also need to contact senior management, patient relations representatives, and technology and communications staff.
- If the breach involves personal health information on an electronic system shared between multiple custodians, be sure to notify them all so that they can conduct their own investigations.

Step 2: Identify the scope of the breach and take the necessary steps to contain it:

- Identify the scope of the breach, including individuals or organizations who may have been involved with or are responsible for the breach, and the nature and quantity of personal health information that is affected.
- Retrieve and secure any personal health information that has been disclosed.
- Ensure that no copies of the personal health information have been made or retained by anyone who was not authorized to receive the information. The contact information of any unauthorized recipients should be obtained in case follow-up is required.
- Determine whether the privacy breach would allow unauthorized access to any other personal health information (e.g., if it involves a shared electronic information system) and take necessary steps, such as changing passwords, identification numbers and/or temporarily shutting your system down.
- In a case of unauthorized access by an agent, consider suspending their access rights.

Step 3: Notify individuals affected by the breach, the IPC, and/or regulatory colleges:

- Identify all affected individuals and notify them of the breach at the first reasonable opportunity. PHIPA does not specify the manner in which notification must be carried out, but in most cases, you should provide direct notification to individuals impacted by a privacy breach by telephone, letter, email or in person. Please refer to appendix 3 for more information about what to include in a breach notification.
- There are exceptional circumstances where custodians may consider using indirect notification to individuals affected by a breach. If your organization is considering indirect notification, you should consult with the IPC. You should be prepared to explain why you believe indirect notice is reasonable in the circumstances and your plans for it. This includes the content of your proposed notice and your strategies for distribution.
- Indirect notice to individuals may be considered by your organization where one or more of these exceptional circumstances apply:
    - The breach affects a significantly large number of individuals, making notifying the affected individuals directly impractical.
    - The risk of harm to affected individuals has reasonably been determined to be low.
    - You are unable to determine the identities of affected parties despite taking reasonable steps to do so.
    - There are questions as to the reliability/accuracy of contact information. Note: Outdated contact information for a portion of the affected parties does not mean that all the affected parties should be notified indirectly. In cases involving a mix of outdated and current contact information, a hybrid approach to notification involving both direct and indirect elements may be appropriate.
    - Direct notification would unreasonably and significantly interfere with the operations of your organization. Note: All breach notification processes will involve the expenditure of time and resources. It is only when the time and resources required to provide direct

notice cause unreasonable and significant interference with your operations that indirect notice may be an option.
    - Direct notification would be reasonably likely to be harmful or detrimental to the affected individuals.
    - For further information on methods of distributing indirect notification to affected individuals, see appendix 3.
- Under PHIPA, custodians must report certain privacy breaches to the IPC at the first reasonable opportunity and cooperate with the IPC. The circumstances that determine if you are required to report the breach to the IPC are set out in the PHIPA regulation and described in detail in the IPC's guidance: **Reporting a Privacy Breach to the IPC: Guidelines for the Health Sector**.
    - If you are required to report the breach to the IPC, do so at the first reasonable opportunity, either **online** or by email or mail.
- If a breach involves an individual who is a member of a regulated health profession, you may be required to notify their regulatory college. This notification is required within 30 days if any of the following applies:
    - The individual was an employee or agent of the custodian and was terminated, suspended, or subject to disciplinary action as a result of a breach.
    - The individual's privileges or affiliation is revoked, suspended, or restricted as a result of a breach.
    - The individual resigns and the custodian has reason to believe that the resignation is related to an investigation or other action carried out as a result of an alleged breach.
    - The individual relinquishes or voluntarily restricts their privileges or affiliation and the custodian has reasonable grounds to believe that it is related to an investigation or other action carried out as a result of an alleged breach.

Step 4: Investigation and remediation

- You will need to conduct an internal investigation to:
    - ensure the immediate requirements of containment and notification have been met
    - review the circumstances surrounding the breach, and
    - review the adequacy of existing policies and procedures in protecting personal health information
    - If you have notified the IPC of a breach, you will be asked to provide the details of your investigation and work with the IPC to identify and commit to any necessary remedial action. You may also be required to cooperate in any IPC investigation related to the breach.
- The process of remediation is critically important to ensure that circumstances that led to a breach can be avoided in future, preventing similar breaches from recurring. This begins

with addressing the conditions of a breach from a systemic basis; in some cases, program-wide procedures may warrant a review.
    - For example, administrative or security controls on an electronic system may be insufficient and need to be updated or augmented.
    - Consider whether all staff have been appropriately educated and trained with respect to compliance with the privacy protection provisions of PHIPA.
- Keeping a log of all privacy breaches can assist in investigations and help to identify systemic issues that may need remediation. You should identify a person responsible for maintaining the log. For each privacy breach, record:
    - the name of the employee or agent that caused the breach, where it is determined to be relevant, such as in the case of unauthorized access
    - the date of the breach
    - the nature, scope, and cause of the breach
    - the number of individuals affected by the breach
    - a description of the PHI that was subject to the breach, and
    - a summary of the steps taken to respond to the breach

For more detailed information about developing privacy breach procedures and responding to breaches, please refer to the IPC guides: **Responding to a health privacy breach: guidelines for the health sector** and **Reporting a Privacy Breach to the IPC: Guidelines for the Health Sector**.

To prepare for the unfortunate risk of a cybersecurity breach, you should seek out reputable cybersecurity firms and experienced legal counsel for guidance in advance, before you find yourself in a crisis. Refer to the IPC fact sheet, **How to protect against ransomware** for additional advice for components that should be included in effective cybersecurity incident management procedures.

Be prepared to report annual breach statistics to the IPC

Also, be sure to maintain a breach log that includes the date (or estimated date) of any breach; a general description of the circumstances of the breach; the kind of information involved in the breach; and whether the breach was reported to affected individuals and the Information and Privacy Commissioner of Ontario.

PHIPA requires custodians to report to the IPC on the number of privacy breaches that occur each year. This report must include all privacy breaches, including those that did not meet the threshold for reporting the breach to the IPC. An accidental privacy breach that is isolated and limited in scope — misdirected correspondence, for example —may not have been reported to the IPC when it happened but should still be counted for annual statistical reporting.

For more information about submitting annual reports, please refer to **Annual Reporting of Health Privacy Breach Statistics to the Commissioner**.

Develop procedures for responding to patient inquiries

Access to information requests

By law, patients are entitled to view and access their personal health information held by health providers at no cost or an amount that does not exceed the amount of reasonable cost recovery. Patients are also entitled to request correction of their personal health information if they believe the records contain inaccurate or incomplete information. You must therefore have procedures in place to respond to such requests, subject to exemptions or exceptions under PHIPA. Your access and correction procedures should cover the following points:

- **The steps people must take if they wish to access their records**. For instance, you may wish to create a standardized form for documenting a request.
- **The timelines for responding to the request**. PHIPA requires you to respond as soon as possible in the circumstances, but no later than 30 days after receiving the patient's request. You may extend this timeline by a further period of up to 30 days under certain circumstances provided you give the requester written notice of the extension, including the length and the reason for the extension. Conversely, you may have to respond in less than 30 days if the requester provides you with evidence that they need access to their personal health information on an urgent basis and you are reasonably able to provide it in that shorter timeframe.
- **Any fees charged for providing copies of the records**. Because of the costs involved in copying the records, you are entitled to charge a reasonable cost-recovery fee. Your procedures should clearly outline how you calculate such fees (see below).
- **Procedures for effective redaction**. If you decide to withhold information that you believe is legally exempted from access or subject to an exception under PHIPA's access scheme, you should have procedures in place for redacting or severing this information, so that the remaining part of the record to which the individual does have a right of access can still be provided to them.

What is reasonable cost recovery?

PHIPA allows you to charge a fee for providing an individual with access to their own personal health information. Because there is currently no regulation that prescribes fees for access, you may exercise discretion in determining the amount to be charged. However, the IPC has the authority to conduct a review to determine whether the fee you charged exceeds the amount of reasonable cost recovery. The IPC has previously concluded that reasonable cost recovery does not mean full recovery of all costs expended in fulfilling an access request.[1]

No more than $30 should be charged for work required to respond to a request, including:

- Receipt and clarification, if necessary, of a request for a record.

[1] IPC **Order HO-009** provides a detailed reasoning for the IPC's conclusions regarding reasonable cost recovery for access.

- Providing an estimate of the fee to be charged.
- Locating and retrieving the record.
- Review of the contents of the record for not more than 15 minutes by the health information custodian or an agent of the custodian to determine if the record contains personal health information to which access or disclosure may be refused.
- Preparation of a response letter to the individual.
- Preparation of the record for photocopying, printing or electronic transmission.
- Photocopying the record to a maximum of the first 20 pages or printing the record, if it is stored in electronic form, to a maximum of the first 20 pages, excluding the printing of photographs from photographs stored in electronic form.
- Packaging of the photocopied or printed copy of the record for shipping or faxing.
- If the record is stored in electronic form, electronically transmitting a copy of the electronic record instead of printing a copy of the record and shipping or faxing the printed copy.
- The cost of faxing a copy of the record to a fax number in Ontario or mailing a copy of the record by ordinary mail to an address in Canada.
- Supervising the individual's examination of the original record for not more than 15 minutes.

In addition to the maximum fees, specific set fees can be charged for certain other services such as photocopying records above 20 pages, printing photographs, and the cost of making or preparing copies of other media such as CDs or USBs, audio or videocassettes, microfiche, X-ray, CT and MRI films.

For more details on what IPC has found constitutes reasonable cost recovery for access, please see IPC **Order HO-009**.

Managing corrections

Patients may dispute the accuracy or completeness of information in their records. If the individual is able to demonstrate, to your satisfaction, that the record is incomplete or inaccurate, and gives you the information necessary to enable you to correct the record, the correction request must be granted.

You should have clear procedures on how to complete a correction in compliance with the requirements under PHIPA. For instance, the individual may require you, to the extent reasonably possible and subject to certain exceptions, to inform anyone to whom the information has been disclosed that there's been a correction. If you do not agree with the correction being proposed, you must have a procedure in place to address that. For instance, under PHIPA, the individual may still require you to attach a statement of disagreement to the record and make all reasonable efforts to disclose the statement of disagreement to anyone who would have been notified had a correction been made.

Please refer to the IPC's **Guide to the Personal Health Information Protection Act** for detailed guidance about responding to correction requests.

Managing complaints and concerns

Patients may have concerns about your information practices. As a custodian, you must have a process to respond to concerns and complaints. Having an accessible and effective complaint management process is an essential aspect of managing privacy risks and helps to promote accountability, openness, and trust. It also allows a practice to address complaints promptly, identify systemic or ongoing compliance issues, and demonstrate a commitment to privacy.

Some steps to consider:

1. Document the complaint/concern including the date it was made
2. Log your response to the complaint and the timing of that response
3. Identify timelines for follow-up and ensure appropriate action has been taken
4. Have an escalation process should the complaint not be easily resolved

Succession Planning

Sometimes changes in personal or professional life can mean changes to your health care practice, and these changes aren't always predictable. However, you should have a clear plan in place for what happens to your practice's health records in the event you retire, move, declare bankruptcy, become incapacitated, or die unexpectedly. Succession planning can ensure that you protect the patients you serve from an interruption to their health care or a breach of their privacy as a result of these changes. It can also protect colleagues, business partners, or loved ones from unexpectedly finding themselves with the cost of having to recover and administer records that you leave behind. Remember, your obligations as a custodian under PHIPA do not end until a legally authorized successor assumes accountability for any records of personal health information that were in your custody or control.

The following best practices should be implemented to prevent abandoned records:

- Create a succession plan that clearly identifies a successor who is legally authorized to hold the records and sets out their responsibilities, and those of any agents (such as a record storage company) who will assist with the retention, transfer, or disposal of records of personal health information
- Ensure the plan identifies a person who will be responsible for:
    - maintaining the security of records
    - responding to patients' access and correction requests
    - making agreements with agents (such as a record storage company) setting out their duties concerning the records
    - notifying patients of the transfer
- Review and update the plan on a regular basis and when there is a change in circumstances that could affect the transfer of those records to a successor

For lessons learned and practical take aways on this topic, see the IPC's case note Lost and found: Preserving abandoned health records.

For additional guidance on this topic, please refer to the IPC publication **Avoiding Abandoned Health Records: Guidance for Health Information Custodians Changing Practice**.

RECAP! Procedures and controls: Key steps to take

- **Get employees to confirm** they will uphold privacy policies.
- **Make sure employees successfully complete annual privacy training.**
- **Review access controls** on a regular basis to limit access to personal health information.
- **Establish good record keeping practices** to keep track of information you may need to reference in the future, such as agreements.
- **Create record retention and destruction procedures** so that records of personal health information are always retained, transferred and disposed of securely.
- **Have a privacy breach response protocol in place** so that you can take immediate action in the event of a breach.
- **Maintain a breach log** to support the reporting of annual breach statistics to the IPC.
- **Develop procedures for responding to patient**s who make access or correction requests, or who have complaints or inquiries about your privacy practices.
- **Establish a business continuity and succession plan** to protect your patients from an interruption to their health care or a breach of their privacy as a result of changes in your personal or professional life.

6.0 Monitoring and review: An ongoing journey

When and how often will you assess your privacy program? How will you know if your agents and service providers are following your policies and procedures? A key step of a successful privacy program is regular monitoring and review.

Why is monitoring and review important?

You've worked hard to put policies, procedures, and controls in place. It's important to check in on a regular basis to ensure that they remain effective so that you stay compliant with your privacy obligations under PHIPA.

Monitoring your program can help prevent surprises, alert you to new privacy risks, keep you on the right side of the law and provide accountability. Here are a few things to consider:

- Is your privacy program functioning as expected?
- How effectively are you and your team complying with PHIPA?
- Are your agents and service providers meeting their contractual obligations around privacy?
- Are your security controls up to date?
- Have there been any changes in privacy laws that are relevant to your practice?

Tips for developing a monitoring and review program

- Continuously monitor your privacy and security controls. Doing so, for instance, will allow you to quickly detect and respond to any new security risks to your data holdings, including any people who are not authorized to access personal health information (e.g., snooping). If you use computers or online applications, consider investing in security monitoring tools or services.
- Establish checkpoints to do an overall program review. This can be monthly, twice a year, or annually. Set intervals that work best for your practice in light of the personal health information you hold.
- Follow up on recommendations arising from privacy impact assessments or privacy audits and ensure they are carried out by their due dates.
- Regularly check expiry dates or renewal requirements of agreements and attestations and put in place a notification system to remind you when it's time to renew them.
- Make sure to terminate access privileges for employees whose employment or contract has ended.

- Also keep your eye on external privacy developments. Laws can change. So too can electronic systems and software, which are frequently updated.
- Document the results of your monitoring activities.
- Adjust your policies, procedures, and controls based on the results of your monitoring and assessments.

RECAP! Monitoring and review: Key steps to take

- **Oversee:** Regularly review your privacy program (once in place) to ensure it remains current and effective and keep good records of your monitoring activities.
- **Monitor:** Depending on your practice, you may need to do more continuous monitoring of your privacy and security controls.
- **Improve:** Use any insights and lessons learned to strengthen elements of your privacy program.

7.0 Appendices

Appendix 1: Sample job description (privacy officer)

An organization's privacy officer is typically delegated with authority to manage all or most aspects of the privacy program on a day-to-day basis. The job description for this role must set out the reporting relationship of the position(s) to organizational leadership and clearly specify the responsibilities and obligations of the position(s) in respect of the privacy program. For most organizations, these responsibilities and obligations would include (but are not necessarily limited to):

- Developing, implementing, reviewing and amending privacy policies, procedures and practices
- Ensuring compliance with privacy policies, procedures and practices implemented by the organization
- Ensuring transparency of privacy policies, procedures and practices
- Facilitating compliance with PHIPA and its regulations
- Ensuring agents are aware of PHIPA and its regulations and their duties with respect to protecting privacy and the confidentiality of records of personal health information
- Ensuring agents are appropriately informed of their duties and obligations with respect to the privacy policies, procedures and practices implemented by the organization
- Ensuring that third party service providers are compliant with contractual privacy obligations by evaluating their adherence to the terms and conditions of agreement at least annually
- Directing, delivering or ensuring the delivery of the initial and ongoing privacy training and fostering a culture of privacy
- Conducting, reviewing and approving privacy impact assessments, as necessary
- Receiving, documenting, tracking, investigating, remediating, and responding to privacy inquiries and complaints
- Receiving, documenting, tracking, and responding to access and correction requests
- Receiving, documenting, tracking, investigating, and remediating privacy breaches or suspected privacy breaches
- Conducting and/or reviewing privacy audits

Appendix 2: Sample privacy policy

Every privacy policy will address the same common elements but should be customized to reflect the specific circumstances of your organization's care model, including the types of personal health information that is collected, the means of collection, the purposes for which it is collected, used, and disclosed. The policy should also reflect the general safeguards that you have implemented to protect individuals' privacy and the confidentiality of personal health information in your custody. You may wish to review the privacy policies of organizations that are similar to yours as possible models to follow.

Statement of principles

Begin with a statement reflecting your commitment to privacy principles, including a commitment to transparency in how your patients' personal health information will be collected, used, and disclosed.

Define personal health information

Use plain language to help patients and other stakeholders understand what kinds of information are subject to the policy. For example, the IPC's **Guide to the *Personal Health Information Protection Act*** states that:

Personal health information includes oral or written information about the individual, if the information:

- relates to the individual's physical or mental health, including family health history
- relates to the provision of health care, including the identification of persons providing care
- is a plan of service for individuals requiring long-term care
- relates to payment or eligibility for health care
- relates to the donation of body parts or bodily substances or is derived from the testing or examination of such parts or substances
- is the individual's health number
- identifies an individual's substitute decision-maker

Any other information about an individual that is included in a record containing personal health information is also included in the definition.

Describe your organization

Explain the structure of your organization, including any relevant business names and a summary of the professional and support staff that may be involved in the patient's care or related administrative functions. Be transparent about your use of any third party service providers that might have access to personal health information in the course of their duties and explain how these relationships are governed.

Describe your purposes for collecting, using, and disclosing personal health information

Clearly explain the different purposes for which you collect, use, and disclose personal health information. For health care organizations, the primary purpose for collecting personal health

information would typically be to provide health care to the individual. You can inform patients that you collect information about their health and their family's health history, current condition and any social determinants of health, in order to assess their health needs, make diagnoses, suggest options, and then provide treatments or other care. Another primary purpose might be to create a current-state record as a reference for future visits that will help you monitor your patient's health over time.

Most health care organizations also collect, use, and disclose personal health information for other valid purposes that may be related to the primary purposes, but are not directly required for the provision of care. You should be clear that you will seek express consent for any purposes that require express consent under PHIPA. Common examples of related purposes are as follows:

- **Payments:** You may need to collect, use, or disclose information to help coordinate payments from your patient or from public or private insurers.
- **Public health:** Some health professionals are legally required to report information that is of public health significance to their local medical officer of health.
- **Quality improvement and risk management:** for the purpose of risk management, error management, or for the purpose of activities to improve or maintain the quality of care, or to improve or maintain the quality of any related programs or services of the custodian.
- **Marketing:** With the express consent of your clients, you might use their information to let them know about services you provide, or to publicize a special event to them.
- **Compliance:** As health care providers, you may be legally required to allow your regulatory college or other regulators to inspect records. Similar reporting requirements may exist requiring you to report information to government agencies. You may also have obligations to report various issues related to professional misconduct or violations of the law.
- **Fundraising:** Fundraising may be permitted with express or implied consent in compliance with PHIPA and its regulation (see **subsection 32 of PHIPA** and **10 of Ontario Regulation 329/04** under PHIPA).

Consent

Clearly explain the circumstances in which you will rely upon:

- **Implied consent**. In many health care settings, a patient's consent to collect or use their PHI is implied by being present and consenting to assessment, diagnosis, or treatment. Health care providers often collect, use, and disclose PHI to consult with other health care providers on the basis of implied consent in the course of providing or assisting in the provision of health care.
- **Express consent**. Explain that there are other circumstances when you need express consent to share information, such as disclosures to persons that are not custodians or to custodians but not for the purpose of health care including for instance, for the purposes of marketing or disclosing to family members or friends, or an insurance company.

Patients should know that they may choose not to give consent, and that consent can be withdrawn at any time, but that this will not have retroactive effect. You should help patients understand how to request a lock-box for some or all of their records.

- **Where consent is not required**: Patients should know that there are circumstances where collection, use, or disclosure of PHI without their consent may be permitted or required by law. For example, subject to the requirements and restrictions, if any, that are prescribed in PHIPA, consent is not required to disclose information to the Minister of Health or another funding custodian so that the minister or the other custodian may determine or provide funding or payment the provision of health care.

Describe the general ways that you protect personal health information

Affirm your commitment to taking the steps that are required to protect personal health information, and provide a high-level explanation of the key technical, physical, and administrative controls that you use, such as (but not limited to):

- Ensuring that paper and digital records are secured in locked or restricted areas when they are not in use.
- The use of strong passwords and role-based access controls for digital systems.
- Ensuring that mobile devices are locked down appropriately.
- Using encryption to protect PHI that is stored or transmitted digitally.
- Training staff members to limit their access to and use of PHI and to act in accordance with the privacy policy.
- Ensuring that all contractors and third party service providers sign agreements with binding requirements to uphold privacy policies.

Describe your retention policy

Clearly explain how long patient records are kept on file and for what reason (e.g., to enable you to answer questions or concerns about those records and to meet any legal requirements).

You should also describe the methods that you use to dispose of personal health information after the retention period. For example, you might use cross-cut shredding to destroy paper files and make digital files irretrievable by overwriting with random data, and/or physically degaussing or destroying hard drives.

Inform patients of their right to access and correct records

The policy should let patients know that they have the right (with few exceptions) to access the records of their personal health information that are in your custody or control and explain how they can make a request to do so. Make sure any requirements for validating identity or documenting the request in writing are clear. Patients should know that you will help them identify relevant records and help them to understand the content of those records (e.g., by explaining acronyms or simplifying technical language). Clarify how you will determine the amount of reasonable cost recovery for providing access.

Similarly, advise patients of their right to request a correction where the record is inaccurate or incomplete (but not to your professional opinions made in good faith). Clearly explain how to document such a request, what evidence will be required, and how you will determine if a correction is appropriate. If you do not agree that a correction is needed, advise patients that their position can be documented in their record. Patients should also know that they may request a

notification to be sent to anyone who had received the information, unless it would not reasonably be expected to have an effect on the ongoing provision of healthcare or other benefit to them.

Describe your breach procedures

Describe what would happen if you discovered a possible loss, theft, or unauthorized access of personal health information in your custody. This would typically include, but is not necessarily limited to:

- Notifying affected individuals, providing your contact information to respond to questions, and providing contact information for the IPC and advising affected individuals of their right to lodge a PHIPA complaint
- Preventing further unauthorized access by changing passwords, restricting access, cutting off networks or shutting systems down
- Taking steps to retrieve any copies of personal health information that might have been disclosed and/or ensuring no copies have been made
- Conducting an investigation
- Taking corrective actions to prevent future breaches (e.g. changes to policies, additional safeguards)
- Notifying and working collaboratively with the IPC, if required
- Reporting disciplinary actions to regulatory colleges

Provide contact information for questions or concerns

Provide contact information for your privacy officer and let patients know that they are available to respond to questions or concerns, or to receive any formal complaints about your privacy practices. Explain your procedure for receiving and addressing complaints, including patients' right to file a **complaint** by contacting:

Office of the Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8
Telephone: (416) 326-3333
Long Distance: 1 (800) 387-0073
www.ipc.on.ca

Appendix 3: Breach notification for affected individuals

Content of a breach notice to affected individuals

- The content of a breach notice should:
  - Provide details of the breach to affected individuals, including the extent of the breach, and what personal health information was involved.
  - Advise all affected individuals of the steps that you are taking to address the breach, and that they are entitled to make a complaint to the IPC. If you have reported the breach to the IPC, advise them of this fact.
  - Provide contact information for someone within your organization who can provide additional information, assistance, and answer questions.
- If financial information is involved, the following statements can be included in the notice:
  - As a precautionary measure, we strongly suggest that you contact your bank, credit card company, and relevant government offices to advise them that you may have been affected by this breach. We recommend you monitor and verify all your bank accounts, credit card and other financial transaction statements for any suspicious activity. If you suspect misuse of your personal information, you can obtain a copy of your credit report from a credit reporting bureau to verify the legitimacy of the transactions listed.
  - Equifax at 1-800-465-7166 or **www.equifax.ca**
  - TransUnion at 1-800-663-9980 or **www.transunion.ca**
  - If you are concerned that you may be a victim of fraud, you may request these bureaus place a fraud alert on your credit files instructing creditors to contact you before opening any new accounts.

The table below provides some suggestions about what to include in a breach notification.

Information to include	Additional comments
Date the breach came to your attention	
Date on which or the period during which the privacy breach occurred	
Description of the breach	*A general description of the nature and scope of the breach, including any potential harms*
The name of the person responsible for the unauthorized access (where appropriate)	
Description of the personal information or personal health information involved in the breach	*Describe the information inappropriately accessed, collected, used, or disclosed.*

Information to include	Additional comments
Description of steps that have been or will be taken to reduce the risk of harm to the affected individual	
Description of steps that have been taken to contain the breach and prevent future breaches	
Steps that affected individuals can take	*Provide information about how individuals can protect themselves, such as contacting ServiceOntario to report a lost or stolen health card number, or contacting credit reporting bureaus to place a fraud alert*
IPC contact information	*If you have already contacted the IPC, include this detail in the notification letter*
Contact information for further assistance	*Contact information for someone within your organization who can provide additional information and assistance and answer questions.*

Distribution of an indirect notice to affected individuals

If it has been determined that an indirect notice is a reasonable approach after assessing the specific circumstances of a breach and consulting with the IPC, the indirect notice must be distributed in a way that could reasonably be expected to reach the affected individuals.

Thought and care should be put into deciding what strategy will be most effective to reach affected individuals. Multiple methods of public notification are generally most effective and are considered a best practice.

A multi-channel public notice strategy should include a combination of some, or all, of the following methods to bring the notice to the attention of the affected individuals:

- A prominent notice on your organization's website or a dedicated website containing details about the breach.
    - If you are using your organization's website to provide notice, ensure the notice or a link to the notice is displayed prominently on the main page of your organizations' website and that it is clearly visible without the need for scrolling or searching.
    - If you are using a dedicated breach website to provide notice, you should place a link to the breach website on the main page of your organization's website so it is clearly visible, and visitors can click through to access the breach website.
    - All digital notices should remain posted for a reasonable period that will allow affected parties to read the notice.

  - Ensure you take reasonable steps to bring the digital notice to the attention of affected parties. Affected parties may be unlikely to visit your website or breach notice unless specifically prompted to go there by media announcements, social media posts, or other means.
- Other public outreach activities to bring the notice to the attention of the affected individuals such as:
  - Posting notices or posters in high traffic areas of your facility for a length of time that will allow affected parties to read the notice.
  - Placing notices in national or local newspapers.
  - Creating social media posts on relevant platforms.
  - Purchasing radio and/or TV announcements and advertising targeted to affected individuals.
  - Issuing news releases and community notices targeted to affected individuals.
  - Hosting town halls and/or webinars to provide information.
  - Any other case-specific public communication strategies that would be effective for reaching individuals affected by the breach.

Appendix 4: IPC resources

Video: IPC FYI is a series of short, engaging videos covering a variety of topics in health privacy available on the IPC's **YouTube** channel.

- **Sharing Health Data**
- **A Guide to AMPs**
- **Understanding PHIPA**

Podcasts: *Info Matters* is a podcast about people, privacy, and access to information hosted by Patricia Kosseim, Information and Privacy Commissioner of Ontario that dives into conversations stories about access and privacy issues. These selected episodes may be of particular interest to the health sector:

- **S1-Episode 10: From the bedside to the board: Building a culture of privacy and security in health institutions**
- **S1-Episode 5: Putting patient trust at the centre of virtual health**
- **S3-Episode 5: Co-designing digital health systems with patients and families**
- **S4-Episode 4: Artificial intelligence in health care: Balancing innovation with privacy**
- **S4-Episode 10: Lessons in health privacy: Key takeaways from 2024**

Cases of Note: Brief summaries of noteworthy orders and cases from the IPC.

- **Ransomware reality: Case study in health care cybersecurity and recovery**
- **Ensuring health data privacy: Insights from the UTOPIAN case**
- **Cyberattack response: Duty to notify individuals under PHIPA and CYFSA**
- **Ensuring secure disposal of health records: Out of sight is not out of mind!**
- **Lost and found: Preserving abandoned health records**
- **Preventing health privacy breaches: Why training, policies and confidentiality agreements matter**

Fact Sheets:

- **Communicating personal health information by email**
- **Succession planning to help prevent abandoned records**
- **How to protect against ransomware**
- **Protect against phishing**
- **Disposing of your electronic media**
- **Health care requirements for strong encryption**
- **Lock-box**
- **Remote work – Working from home during the COVID-19 pandemic**
- **Fundraising under PHIPA**

Guidance:

- **A guide to the Personal Health Information Protection Act**
- **Circle of care: Sharing personal health information for health-care purposes**
- **Detecting and deterring unauthorized access to personal health information**
- **Privacy and security considerations for virtual health care visits**
- **Frequently asked questions: Personal Health Information Protection Act**
- **Use and disclosure of personal health information for broader public health purposes**
- **Digital health under PHIPA: Selected overview**
- **Responding to a privacy breach: Guidelines for the health sector**
- **Reporting a privacy breach to the IPC: Guidelines for the health sector**
- **PHIPA breaches workbook and completion guide**
- **Safeguarding privacy on mobile devices**
- **Avoiding abandoned health records: Guidance for health information custodians changing practice**
- **De-identification guidelines for structured data**
- **Planning for success: Privacy impact assessment guide**
- **Privacy impact assessment guidelines for the Ontario *Personal Health Information Protection Act***
- Procuring, implementing, and using AI Scribes: Key considerations for the health sector

A Privacy Management Handbook for Small Health Care Organizations

Information and Privacy Commissioner of Ontario

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

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

www.ipc.on.ca
416-326-3333
info@ipc.on.ca

May 2025