Yukon
Information
and Privacy
Commissioner

3162 Third Avenue
Whitehorse, Yukon Y1A 1G3
T: 867 667 8468
F: 867 667 8469
Toll free: 1 844 997 8468
YukonIPC.ca

HIPMA Guide for Small Custodians

Supporting your obligations to the *Health Information Privacy and Management Act*

February 2026

Table of Contents

Disclaimer: This guide is for informational purposes only and does not constitute legal advice. Refer to HIPMA for a complete understanding of your obligations.

HIPMA Guide for Small Custodians

This interactive guide is designed to help small custodians and their agents understand and comply with their obligations under Yukon's Health Information Privacy and Management Act (HIPMA). The Department of Health and Social Services or the Yukon Hospital Corporation are not small custodians and have different obligations.

In addition to compliance obligations, this guide contains information like HIPMA terminology, fillable templates, sample forms, and additional resources to help you navigate the Act. We recommend that you fill out Appendix A, B, and C as you read this guide. Appendix A will form the basis of a custodian's privacy and access policy and procedures, Appendix B is a sample statement of practice, and C is a sample consent notice.

Health sector access and privacy legislation

Health Information Privacy and Management Act (HIPMA)

The purpose of Yukon's HIPMA is to establish strong and effective mechanisms to protect personal health information, establish rules for the collection, use, disclosure, security, and management of personal health information, and provide individuals with the right to access their personal health information or request the correction of inaccuracies.

HIPMA applies to custodians, and their agents who collect, use, or disclose personal health information (PHI) for the purposes of providing health care and for the planning and management of the health system or research. A HIPMA glossary is located on page 19.

Personal Information and Protection of Electronic Documents Act (PIPEDA)

Most Yukon custodians are also subject to the federal privacy legislation known as PIPEDA. PIPEDA applies to the collection, use, and disclosure of personal information for specified purposes. The Office of the Privacy Commissioner of Canada is an excellent resource on PIPEDA and its application. HIPMA was designed to be substantially similar to PIPEDA, so compliance with HIPMA, likely means compliance with PIPEDA.

Structure and operations

It is essential for a custodian to review their structure and operations to ensure they are compliant with HIPMA. The custodian must be identified, and if applicable, their agents, information managers, and contact individual(s).

Template A and sample policies and procedures are included to help ensure compliance. If all fields are completed in sufficient detail, this template can become the basis for a custodian's access and privacy policies. We suggest you keep the template handy and fill it out as you go through this guide.

Identifying the custodian(s)

[Insert your answer into the template]

A custodian is the health care provider responsible for making decisions and overseeing operations.

Custodians may include:

- medical practitioners;
- registered nurses or nurse practitioners;
- licensed practical nurses;
- pharmacists;
- chiropractors;
- optometrists;
- dentists;
- members of a designated health profession such as physiotherapists; and
- the operator of a health facility.

In addition to the list above, custodians include:

- physicians operating a private practice, and/or professional corporation;
- owners of a pharmacy; or
- psychologists, physiotherapists, dentists, etc. operating a private practice.

Our office can help with custodian identification if there is uncertainty.

Identifying the agent

[List agents on the template]

Agents are people who act for or on behalf of the custodian and can include:

- medical office assistants;
- office managers;
- reception/front desk staff;
- volunteers; and
- trainees and students.

A custodian can have multiple agents! Agents must sign a pledge of confidentiality acknowledging they are bound by HIPMA and are aware of the consequences of a breach.

Identifying information manager(s)

[List your information manager(s) on the template]

Information Managers are individuals who act for or on behalf of the custodian for the purposes of data management and information technology services, including:

- processing, storing, retrieving, archiving, or disposing of information; and
- striping, encoding, transforming identifying information to create non-identifying information.

Examples:

- If you use an electronic medical records management system (EMR), this service provider is your information manager (e.g., Plexia, Canadian Health Systems, etc.).
- If a company manages your IT infrastructure and office computer network, they are your information manager.
- If a shredding company disposes of your records, they are your information manager.

Information managers are a type of agent that has additional requirements that must be met. It is possible to have more than one information manager.

You must have a written agreement with your information manager(s).
For more information, see the section on Custodians and information managers (page 11)

Identifying contact individuals

[List your contact individual(s) on the template]

Custodians must designate a contact individual or they automatically become the contact individual (subsections 20 (1) and (3)). An agent can be a designated contact individual.

The obligations of a custodian's designated contact individual include (Subsection 20 (2)):

- receive and process complaints from the public about the custodian’s information practices;
- respond to requests for access to, or correction of, a record of an individual’s personal health information that is in the custody or control of the custodian (sections 24 through 28);
- ensure that all agents of the custodian are appropriately informed of their duties under this Act;
- respond, in respect of security breaches, to individuals whom the custodian has notified under section 30 and to the IPC; and
- perform any prescribed functions or duties. **

**Section 16 of the *Health Information General Regulations* outlines that the functions and duties of a custodian's contact individual include:

- facilitating the custodian's compliance with the Act;
- assisting individuals in the making of complaints in relation to the custodian, including complaints to the IPC; and
- facilitating the education and training of the custodian's staff regarding the Act and the custodian's information practices.

Obligations under HIPMA

Custodians must properly manage their agents, information managers, and contact individuals to ensure compliance with HIPMA.

Collection, use, and disclosure in accordance with HIPMA

A person who is a custodian or the agent of a custodian may collect, use, disclose and access personal health information only in accordance with HIPMA and the regulations (section 13).

See the definitions for collect, use, disclosure, registration information and personal information in the glossary.

If you have an agent! Agents can only collect, use, disclose, or access PHI if the custodian has explicitly permitted them to do so. For more information on this, see the section on Custodian's Information Practices on page 12.

Limited collection, use, or disclosure (limitation principal)

The custodian and their agent must limit their collection, use, and disclosure of personal health information to the minimum amount that is reasonably necessary to achieve the purpose of providing health care to the individual (section 16).

The Limitation Principle is a fundamental component of HIPMA - a "need to know" principle.

If you have an agent, the limitation principle also applies to agents, and a custodian is responsible for ensuring the agent understands and complies with it.

Start by considering what information you are collecting from your patients and evaluate whether you need the information to provide health care to that patient.

The following are some examples to help you evaluate your practices in respect of collection and disclosure.

Example 1: Am I collecting too much information?

Jenny is a new patient of Dr. Grant. At her first appointment, she is asked to fill out a health questionnaire and provide some basic information. While most of the questions make sense (allergies to medications, chronic health conditions, etc.), Jenny wonders why Dr. Grant needs her partner's name and phone number, or why she is being asked to provide her employer's name and address.

It is not clear how this information relates to the provision of health care and therefore collecting it **may be contrary to HIPMA.**

If you determine that you do need to collect this information to provide health care to Jenny, then be clear about **why** you are collecting it.

For example, if you are collecting the partner's name and phone number as an emergency contact, then specify this on the form and let the patient decide who to choose.

If you don't need the information, don't collect it!

In this example, Dr. Grant is collecting contact information about another individual, Jenny's partner, from Jenny. This is an indirect collection of the partner's information. HIPMA has rules about collecting personal health information indirectly. These rules are contained in section 54.

Example 2: Am I disclosing too much information?

You are Steve's psychiatrist, and his family doctor has requested a status update, so you have your medical office assistant send a copy of Steve's complete medical records to his family doctor.

Disclosing Steve's complete medical file to his family doctor **may be contrary to HIPMA** as it is unclear why his family doctor would require this level of detailed and sensitive personal health information.

In this example, it might be more appropriate to send the family doctor a high-level summary including your diagnosis and any medications you have prescribed. This disclosure is likely reasonable in the circumstances.

If Steve's family doctor insists on receiving additional information beyond this, then it is best to inquire about why the family doctor needs this information, **before** disclosing Steve's sensitive personal health information.

As well, remember to ensure that Steve consents to the disclosure, or that you have authority to disclose the information without consent.

Consent

HIPMA is consent-based legislation and generally requires that custodians obtain a person's consent to collect, use, or disclose their PHI.

If the custodian is required by the Act to obtain consent to collect, use, or disclose PHI, it must follow the rules for consent in sections 32 to 47.

Consent must meet certain requirements for the purpose of providing health care. Namely, consent must be "knowledgeable." The individual must know the purpose of the collection, use, or disclosure of the PHI, that they may give or withhold consent, and that their PHI can be collected, used or disclosed without their consent only in accordance with the Act and its regulations (section 39).

Document consent. It is recommended that custodians always document patient consent. For example, if consent was obtained verbally, it should be noted on the patient's file. Without documentation, custodians cannot substantiate that an individual's consent was obtained. This practice promotes transparency and accountability in the provision of health care.

Recording requirements for disclosures without consent

HIPMA allows for disclosure of PHI without patient consent in certain circumstances. Section 58 of HIPMA lists the circumstances in which a custodian may disclose PHI without consent. Disclosure of PHI under this section is discretionary.

If PHI is disclosed without consent in accordance with section 58, the details of the disclosure must be recorded in accordance with subsection 22 (1). These details must include their name, the date and purpose of the disclosure, and a brief description of the personal health information. This **does not apply** to the disclosure of a record that contains only registration information or provider registry information.

Consent through notice

Under HIPMA, custodians may rely on a "notice" for obtaining knowledgeable consent to collect, use, or disclose an individual's PHI. The notice must meet the requirements of subsection 41 (1) of HIPMA and section 17 of the *Health Information General Regulation*.

The consent notice must:

- be in writing;
- be expressed in plain language; and
- describe the custodian's record retention schedule.

Obtaining knowledgeable consent might be best achieved through a combination of a notice establishing a baseline of knowledgeable consent, and ongoing communication between the physician and patient in respect of providing them with care.

Frontline staff could proactively refer individuals to the posted privacy notice as part of any discussion with a new patient. Patients should be offered the opportunity to ask questions about the notice. Ensure that frontline staff have sufficient training to answer general questions about your information practices.

Record of user activity

HIPMA requires a custodian to maintain a **record of user activity** in respect of any electronic information systems used by the custodian – for example, the electronic medical records management system (EMR).

A record of user activity must include:

- the person's identification (e.g., employee ID #);
- the date of the incident (when the PHI was accessed); and
- a description of the information that is accessed or that could have been accessed.

All electronic systems must have a record of user activity (access log) of who accessed what PHI, and when.

If your electronic information system is not currently meeting this requirement, you should contact the service provider to determine if this feature can be activated. If not, then you should consider switching to a system that meets this requirement as failing to do so would be contrary to HIPMA**.**

Custodians and information managers

A custodian who proposes to retain the services of an information manager must (subsection 51 (1)):

> *(a)* ***enter into a written agreement*** *with the information manager that provides for the protection of the information that is the subject of the services; and*
>
> *(b) comply with the prescribed requirements, if any.*

Section 21 of the *Health Information General Regulation* specifies the requirements of the written agreement with an information manager.

The requirements for written agreements with information managers are quite extensive, and as such, you may want to consider retaining a lawyer to assist in drafting the agreement to ensure compliance with HIPMA and the regulation.

If you already have an agreement in place with your information manager, you may consider having a lawyer review it to ensure it meets all the requirements.

Custodian information practices

A custodian must protect PHI by applying information practices that include administrative policies and technical and physical safeguards that ensure the confidentiality, security, and integrity of the personal health information in its custody or control (Subsection 19 (1)). Subsections 19 (2) and (3) identify the standards for protection and specific controls required to meet subsection 19 (1).

The custodian is responsible for the organization's compliance with HIPMA including that of their agents and information managers. Ongoing **training** and implementing comprehensive **written policies and procedures** are the best ways to ensure agents and information managers know and understand their obligations under HIPMA.

Custodians must ensure they are adequately always protecting patient PHI. Safeguards must be proportionate to the sensitivity of the information. This requires establishing what PHI is in your custody or control and then determining how best to protect it, paying particular attention to PHI that is sensitive in nature.

There is no "one-size-fits-all solution" for meeting your obligations under HIPMA and the threshold for what is an adequate safeguard may differ between custodians.

For example, a psychologist may have more sensitive PHI in their custody or control than a dentist, and therefore more stringent safeguards may be necessary.

Evaluate and document your office's compliance using the Access and privacy policy and procedures template (Appendix A).

Administrative policies include written policies outlining the custodian's instructions in respect of collecting, using, and disclosing PHI and the rules to effectively safeguard the PHI; breach reporting procedures; and ongoing privacy and security training for employees.

Technical and physical safeguards.

- Access controls restrict the PHI that employees can access. They can be administered through electronic medical records management systems (EMR) and can limit snooping and other unauthorized access to PHI. It is particularly important to limit access to sensitive PHI. Different agents may require different levels of access to PHI. For example, consider whether it is appropriate for your reception staff to have full access to all patient medical records.

EMR systems must be able to verify the identity of the person accessing the PHI and keep a record of user activity, in order to comply with HIPMA. This can be done by the following:

- locks on doors and filing cabinets, and rooms with restricted access
- regularly monitoring or auditing EMR systems to detect potentially unauthorized accesses by employees (snooping)
- using a secure file transfer platform for electronically sending and receiving records containing PHI - unencrypted email is not a secure method for electronically sending and receiving such records
- encryption of servers, workstations, mobile devices and other data carriers used to access and store PHI
    - adequate methods of authentication, including two-factor authentication for accessing EMR systems
- physical security might include a monitored alarm system, or electronic "fob" / access cards for gaining access to the premises
- confidentiality might include soundproofing exam rooms to limit eavesdropping, or a confidential area at reception where patients can speak privately. Training should include locking screens when leaving a workstation and making sure paper files are not left in sight of the public or unauthorized employees.

If you have an agent! Section 14 of the *Health Information General Regulation* outlines how your information practices apply to your agents:

- agents cannot access PHI unless the custodian has determined and outlined what PHI they are authorized to access;
- agents must sign a pledge of confidentiality acknowledging they are bound by the Act and are aware of the consequences of a breach; and
- the agent, if appropriate, was provided with privacy and security orientation training by the custodian.

Mandatory bi-annual audit requirement

Custodians are required to "*…at least every two years, conduct an audit of the custodian's security safeguards, including their information practices and procedures*", according to paragraph 14 (1)(c) of the *Health Information General Regulation*." Paragraph 14 (1)(d) requires a custodian to *"as soon as possible, identify and address any deficiencies identified in an audit.*"

The IPC published an audit tool to help custodians evaluate their safeguards and information management practices under HIPMA. The results of this audit should be time-stamped and stored for compliance purposes as you may be required to produce this record as part of investigations or compliance review by the IPC.

Statement of practice

A custodian must make available to the public a written statement that provides (section 21):

- a general description of its information practices;
- information on how to reach the custodian's contact individual;
- a description of how an individual can obtain access to, or request a correction of their personal health information; and
- a description of how to make a complaint to the custodian, and to the IPC.

Use template Appendix B to create your organization's statement of practice.

Security breaches and notification of individuals

A security breach means that PHI was accessed, stolen, lost, disclosed, or disposed of contrary to HIPMA. Breaches can result from malware, an employee who purposely or accidentally discloses patient PHI, missing laptops, mobile devices, or physical records.

HIPMA has mandatory breach notification provisions. As such, custodians should carefully review the provisions noted below and be sure they understand their obligations in respect of security breaches.

Custodians **must notify an individual** about a breach of their PHI if there is a **risk of significant harm** to that individual, as outlined in subsection 30 (1). The risk is based on the sensitivity of the information involved in the breach.

Significant harm includes risk of bodily harm; humiliation; damage to reputation or relationships; loss of employment, business or professional opportunities; financial loss; identity theft; negative effects on their credit record; and damage to or loss of property.

Next, the custodian must determine if there is a possibility that the individual may be exposed to or suffer from significant harm. The custodian should consider the factors outlined in paragraphs 30 (3)(a) through (g) of HIPMA to make this determination.

Subsection 30 (2) outlines the requirements of notifying an affected individual of a security breach. If custodians notify the affected individual, they must also notify the Information and Privacy Commissioner (IPC) **with** a copy of the notice to the individual and a written report. See subsection 31 (1) for the requirements of the report to the IPC.

If you have an agent/information managers! Custodians should have clear breach reporting protocols for their organization. It is imperative that your agents/information managers know what constitutes a security breach, who to report it to, and to do so immediately to minimize the risk of significant harm.

Security Breach?

Frank is at the dentist for his routine check up. Margaret, the dental hygienist, pulls up Frank's x-rays on the computer screen next to the dental chair to discuss what they found. Margaret then pulls up the clinic's calendar on the screen to book Frank's next appointment. The phone rings, and Margaret leaves the room for a moment forgetting to lock the computer screen. She returns a few seconds later to find Frank browsing the scheduled appointments of other patients on the screen. Frank comments *"Hey, my neighbor comes here too!"*

While the Margaret's mistake was unintentional, Frank has accessed other individuals' personal health information without authority.

This is a security breach.

Now What?

Margaret locks the screen and informs Frank that this constitutes a privacy breach as he was not authorized to view this information. Margaret explains that she will need to report the incident to the dentist (the custodian) who may need to follow up with him later to discuss the details of what happened.

She asks Frank to confirm whether he viewed any other information beyond what was immediately visible on the screen and to confirm whether he recognized or knew any of the other people whose appointments he viewed.

Margaret takes a screen shot of the information viewed by Frank so there is a record of what information was accessed without authority.

She immediately reports the incident to the custodian as outlined in the clinic's breach reporting procedure for which she receives yearly training.

Risk of significant harm?

The custodian reviews the information that was breached to assess whether there is a risk of significant harm to any of the individuals whose PHI was viewed by Frank. As well, the custodian contacts Frank directly to corroborate the information about the breach as provided by Margaret and obtains Frank's assurance in writing that he will not divulge the contents of the record he accessed.

After considering the information that was breached (names and appointment dates), the factors above and those outlined in paragraphs 30 (3)(a) through (g) and determining through access logs that Frank did not access any other information, the custodian determines there is no risk of significant harm to any of the individuals as a result of the breach. As such, it is not necessary to formally notify the individuals in accordance with section 30 (2).

Despite that there is no requirement to do so, the custodian decides to contact each of the individuals whose PHI was breached to explain what happened and what measures will be taken to avoid a recurrence going forward.

The dentist reminds Margaret about the requirements to lock her computer anytime she is away from her desk and commends her for her diligence in having recognized, mitigated, and reported the breach right away!

Evaluation of a security breach is contextual. In the above example, had the breach involved the records of a psychiatrist, it is likely that a risk of significant harm would be found because the mere fact that Frank knows his neighbour is seeing a psychiatrist can cause the neighbour harm.

Most breaches are inadvertent, but this does not mean they are not serious. It is important that your agents feel comfortable recognizing and reporting breaches.

All breaches have the potential to adversely affect individuals and therefore need to be identified and assessed as quickly as possible – this cannot happen unless they are reported!

Transferring patients and succession planning

Custodians who may transfer their patients to another custodian, retire, leave the territory, or otherwise cease their operations need to consider Continuing Duties of Custodians (section 23).

The custodian's duties with respect to PHI, **apply until they transfer custody and control of the PHI or the records to a successor (section 60)** or to a prescribed person in accordance with the prescribed requirements.

The obligations for disclosing PHI to a successor custodian includes an **agreement to relinquish the custody and control** of PHI and making reasonable efforts to give notice to individuals before transferring their PHI to the successor (section 60).

Succession Plan: In the absence of a succession plan, and a custodian *"becomes incapable of managing their affairs, or dies"* the custodian's *"guardian"* or *"personal representative"* is **deemed to be a custodian** and **must** carry out the responsibilities of the custodian, including transferring any records to a successor custodian (subsection 3 (2)). Without a plan in place, this duty could fall to a spouse, adult child, or other family members. To avoid this, you should consider identifying a successor custodian and have a succession plan in place.

Request for access and correction of PHI

Individuals have a right to access their personal health information with limited exceptions. Sections 24 to 28 govern this process, including how individuals can request their PHI.

Written procedures should be established for managing access requests, and custodians must ensure that all the requirements are met including:

- statutory timelines for responding to access requests;
- time extensions;
- contents of the response;
- how access is to be granted;
- refusing access;
- fees;
- notifying applicants if their PHI is in the custody or control of another custodian; and
- managing requests for correction of an individual's PHI.

Glossary

Agent *of a custodian means a person (other than a person who is prescribed not to be an agent of the custodian) who acts for or on behalf of the custodian in respect of personal health information, including for greater certainty such a person who is:*

(a) an employee of the custodian;

(b) a person who performs a service for the custodian under a contract or agency relationship with the custodian;

(c) an appointee, volunteer or student;

(d) an insurance or liability protection provider;

(e) an information manager;

(f) if the custodian is a corporation, an officer or director of the corporation; or

(g) a prescribed person.

Collect *means to gather, acquire, receive or obtain by any means from any source, but does not include the transmission of information between a custodian and an agent of that custodian.*

Consent *where the context permits, includes the power to give, refuse and withdraw consent.*

Custodian *means a person (other than a person who is prescribed not to be a custodian) who is:*

(a) the Department of Health and Social Services;

(b) the operator of a hospital or health facility;

(c) a health care provider;

(d) a prescribed branch, operation or program of a Yukon First Nation;

(e) the Minister;

(f) a person who, in another province:

(i) performs functions substantially similar to the functions performed by a health care provider, and

(ii) is, in the performance of those functions, subject to an enactment of Canada or a province that governs the collection, use and disclosure of personal information or personal health information, or

(g) a prescribed person.

Disclose *means, in relation to information in the custody or control of a person, making the information available or releasing it to another person, but includes neither using the information nor its transmission between a custodian and an agent of that custodian;*

Health care *means any activity (other than an activity that is prescribed not to be health care) that is or includes:*

(a) any service (including any observation, examination, assessment, care, or procedure) that is provided

(i) to diagnose, treat or maintain an individual's physical or mental condition;

(ii) to prevent disease or injury or to promote health;

(iii) as part of rehabilitative or palliative care; or

(iv) for any prescribed purpose.

(b) the compounding, dispensing or selling of a drug, a device, equipment or any other item for the use of an individual pursuant to a prescription where a prescription is required by law.

Health care provider *means*

(a) a medical practitioner;

(b) a registered nurse or nurse practitioner;

(c) a licensed practical nurse as defined in the *Licensed Practical Nurses Act*;

(d) a pharmacist;

(e) a chiropractor as defined in the *Chiropractors Act*;

(f) an optometrist;

(g) a dentist;

(h) a dental assistant, dental therapist or dental hygienist, as those terms are defined in the *Dental Profession Act*;

(i) a denturist;

(j) an individual who is a member of a designated health profession as defined in the *Health Professions Act*;

(k) a professional corporation entitled to practice health care through or on behalf of an individual listed in paragraph (a) through (j); or

(l) a prescribed person.

Health facility *means*

(a) a medical clinic, community health centre, dental clinic, medical laboratory, specimen collection centre or pharmacy;

(b) a clinic or facility in which health care diagnostic testing or health care procedures are routinely provided;

(c) a residential facility, including a nursing home, that provides continuing health care or long-term health care; or

(d) a prescribed facility.

Health information *of an individual means identifying information of the individual, in unrecorded or recorded form, that:*

(a) relates to the individual's health or the provision of health care to the individual;

(b) relates to payments for health care;

(c) relates to the donation by the individual of any body part, tissue or bodily substance of the individual;

(d) is derived from the testing, including genetic testing, or examination of any body part, tissue or bodily substance of the individual; or

(e) is prescribed.

Information manager *means a person (other than a person who is prescribed not to be an information manager) who, for or on behalf of a custodian:*

(a) processes, stores, retrieves, archives or disposes of information;

(b) strips, encodes or otherwise transforms identifying information to create information that is not identifying information;

(c) provides information management or information technology services; or

(d) provides a prescribed service.

Personal health information *of an individual means*

(a) health information of the individual; and

(b) except as prescribed, prescribed registration information and prescribed provider registry information in respect of the individual.

Personal information *has the same meaning under HIPMA as it does under the Access to Information and Protection of Privacy Act (ATIPP Act).*

Personal Information means recorded information about an identifiable individual, including:

(a) the individual's name, address, or telephone number;

(b) the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations;

(c) the individual's age, sex, sexual orientation, marital status, or family status;

(d) an identifying number, symbol, or other particular assigned to the individual;

(e) the individual's fingerprints, blood type, or inheritable characteristics;

(f) information about the individual's health care history, including a physical or mental disability;

(g) information about the individual's educational, financial, criminal, or employment history;

(h) anyone else's opinions about the individual; and

(i) the individual's personal views or opinions, except if they are about someone else.

Registration information *of an individual means the individual's:*

(a) name, including any previous names;

(b) gender;

(c) date of birth;

(d) place of birth;

(e) date of death;

(f) residential address;

(g) telephone number;

(h) email address;

(i) personal health number issued by a province or Canada for the purpose of providing health services to the individual;

(j) unique identifier, if any, assigned by a custodian's information system in order to identify the individual; and

(k) substitute decision-maker's name, residential address and telephone number, if the individual has a substitute decision maker.

Security breach *means, with respect to personal health information*

(a) theft or loss; or

(b) disposition or disclosure, or access by a person, contrary to this Act or a regulation.

Use *includes, in relation to personal health information in the custody or control of a person:*

(a) handling or dealing with the personal health information in any manner whatever, other than by collecting or disclosing it; and

(b) the transmission of personal health information between a custodian and an agent of that custodian.

Appendix A –Access and privacy policy and procedures template

This template is intended to help small custodians develop and/or evaluate their organization's compliance with HIPMA. If used correctly and completed in sufficient detail, this document can serve as the basis for an organization's access and privacy policy and procedures.

HIPMA governs the collection, use, disclosure, security and management of personal health information, and provides individuals with the right to access their personal health information or request the correction of inaccuracies.

Information practices: This policy and associated procedures templates outlines the circumstances in which the custodian will collect, use, disclose, access, and manage the personal health information of individuals.

Principles for the custodian to consider:

- manage personal information in a privacy-protective manner in compliance with HIPMA
- an individual has the right to the protection of their PHI that is held by the custodian and has the right to access it and to correct inaccuracies
- transparency in how it protects PHI that it holds
- obligation to notify an individual if there is a breach of their PHI that results in a risk of significant harm to the individual
- continual evaluation of its information practices to ensure compliance with HIPMA

Appendix A –Access and privacy procedures template

Structure and operations:

Who is the custodian?	Things to consider…
	If identifying the custodian is not immediately obvious to you, a more thorough evaluation may be required. You can contact our office for further guidance on making this determination.
Who are your agents?	**Things to consider…**
List your agent(s)	*Agents may include employees, contractors and volunteers. An agent is any person that you have expressly authorized to collect, use, disclose or access PHI for you or on your behalf.*

Appendix A –Access and privacy procedures template

Who is your information manager(s)?	Things to consider…
List your information manager(s)	*Remember there may be more than one!* *Written Agreement requirements (section 21)* *You need to have a written agreement in place with all your information managers and meet the requirements under HIPMA. See Custodians and Information Managers.* *You may want to attach a copy of any agreements to the end of this document for ease of reference.*
Who is your contact individual? (s. 20)	**Things to consider…**
	You must designate a contact individual, which could also be an agent. ***If you do not make a designation, the custodian is deemed to be the contact individual.*** *Ensure your contact individual knows and understands their obligations outlined in subsection 20 (2) and section 16 of the Regulation.* *Your contact individual is responsible for several duties, including:* • *receiving and managing complaints from the public about your information practices* • *responding to requests for access or correction of PHI* • *ensuring that all agents are appropriately informed of their duties under HIPMA* • *responding to security breaches*

	Your contact individual must also be trained to make decisions about the authority to collect, use or disclose personal health information that is not specified in your policy and procedure.
Electronic information systems (s. 22 (3))	Things to consider…
List the electronic system(s) you use to store PHI including their location. For example, your electronic medical records management system (EMR). Include how user activity is recorded.	*A **record of user activity** means:* • *the person's identification (e.g. employee ID #)* • *the date of the incident (when the PHI was accessed)* • *a description of the information that was accessed or that could have been accessed.*

Appendix A –Access and privacy procedures template

Custodian's obligations:

Collection, use, and disclosure	Things to consider…
*What personal health information (PHI) do you normally **collect** and why?* *When describing the PHI in this section, you may wish to categorize the information. For example, I collect PHI from individuals only as necessary to provide them with health care. I collect health insurance information for billing purposes.*	*Collection, use and disclosure must only be in accordance with HIPMA (s.13).* *You must limit the amount of PHI collected, used, and disclosed to the minimum amount reasonably necessary to achieve the intended purpose. **The limitation principle is fundamental to HIPMA and needs to be factored into every facet of your operations.*** ***Evaluate what PHI you regularly collect, use and disclose.*** *Review forms, questionnaires, etc. Consider the circumstances when you regularly use and disclose patient PHI. (e.g., referrals to another custodian, patient changing doctors, etc.)* ***Training?*** *Do your agents understand the limitation principle?*
*What PHI do you normally **use** and why?* *For example, I use a patient's PHI when providing them with health care and for communicating with my office staff (agents) for follow-up as necessary to provide the patient with ongoing health care.*	

Appendix A –Access and privacy procedures template

*What PHI do you normally **disclose** and why?* *For example, I disclose billing information to receive payment. I disclose PHI to another custodian or care provider only as necessary to facilitate the ongoing care of my patient.*	
Consent (s. 39)	Things to consider…
How does your organization typically obtain knowledgeable consent from patients?	*Generally, patients should be kept informed in respect of the collection, use or disclosure of their PHI to allow them to make informed decisions about their care.* *Under HIPMA, custodians may rely on a notice for obtaining knowledgeable consent to collect, use or disclose an individual's PHI. The notice must meet the requirements of subsection 41 (1) of HIPMA and section 17 of the Health Information General Regulations.* ***TIP!** Obtaining knowledgeable consent might be best achieved through a combination of a notice establishing a baseline of knowledgeable consent, and*

	ongoing communication between the physician and patient in respect of providing them with care. *Consider having frontline staff proactively refer individuals to the posted privacy notice as part of any discussion with a new patient. Also, patients should be offered the opportunity to ask questions about the notice.* *Consider ensuring that frontline staff have sufficient training to answer general questions about your information practices.*

Recording requirements (s. 22)	Things to consider…
Detail how your organization will meet the recording requirements under s.22 of HIPMA.	*When disclosing PHI **without consent**, you must document:* - *the name of the person to whom you disclosed the PHI;* - *the date and purpose of the disclosure; and* - *a brief description of the PHI disclosed.* ***Is this being done?*** ***Are your staff aware of this requirement?***

	Section 58 outlines the circumstances in which a custodian can disclose personal health information without consent.

Custodian's information practices (s. 19):

Technical, administrative and physical safeguards	Things to consider…
Detail your organization's administrative and technical safeguards.	*Evaluate whether your safeguards are adequate to protect the PHI under your custody and control.* *Some examples include:* - *a policy regarding the safe and appropriate usage of the custodians' systems and the PHI contained in the systems;* - *ongoing training of employees and agents regarding information security and privacy practices;*

	- *a controlled termination of employment process to ensure that any outgoing employees no longer have access to any records, electronic systems, or to the premises. The employee's accesses should be removed prior to termination;* - *access controls for paper and electronic records;* - *logging and auditing of your EMR to detect unauthorized activity by employees (e.g. snooping, unauthorized alteration of data, etc);* - *using a secure method of transmission for sending/receiving documents (e.g. secure file transfer);* - *encryption of servers and other data carriers;* - *proper authentication, including two-factor authentication for EMR systems.*
Physical security	**Things to consider…**
Detail the security measures your organization has in place.	*Some examples include:*

	- *locks on doors, filing cabinets and restricted areas;* - *a monitored alarm system; or* - *electronic fob/access cards for gaining access to the premises.*
Confidentiality	Things to consider…
Detail how your organization keeps PHI confidential.	*Some examples include:* - *sound-proofing rooms to limit eavesdropping or a confidential area at reception where patients can speak privately;* - *ensuring computer screens are locked automatically when inactive and training employees to lock screens when leaving their workstation; and* - *training staff to ensure paper records are not left unattended*

Appendix A –Access and privacy procedures template

Security breaches and notifications (s. 30, 31)	Things to consider…
Detail your organization's procedure for managing a security breach	*HIPMA has mandatory breach notification provisions so it is important you take the time to understand your obligations.* *Your organization should have clear breach reporting protocols so your agents know what constitutes a breach, who they should report it to, and that they must do so immediately.* *Your procedures should outline measures to identify and contain security breaches, as well as the notification of individuals affected by real or suspected security breaches. It should identify roles and responsibilities to effectively respond to breaches quickly and in a coordinated manner.* *Your designated contact person should be identified as the person responsible to receive breach reports and for managing the breach process to ensure HIPMA's mandatory breach reporting requirements are met.*

Appendix A –Access and privacy procedures template

Transferring patients (s. 23, 60)	**Things to consider…**
Detail your organization's procedure for transferring patient records to a successor custodian.	*These sections are particularly important if you are thinking of transferring patients to another custodian, retiring, or leaving the territory, or otherwise ceasing operations.* *Disclosing PHI to a successor custodian* ***requires an agreement*** *that you relinquish the custody and control of PHI and requires you to make reasonable efforts to notify individuals* ***before*** *transferring their PHI to the successor.* *You may want to consider identifying a successor custodian now, in case something unexpected happens to you.* *If you do not identify a successor custodian, the duty to transfer your patient files to a successor custodian may fall to your spouse, adult child, or other family member.*

Appendix A –Access and privacy procedures template

Request for access and correction of PHI (s. 24 to 28)	Things to consider…
What is your organization's process for managing access requests or requests to correct PHI?	*individuals have a **right to access their PHI,** with limited exceptions. Sections 24 through 28 of HIPMA govern this process including how individuals can request their PHI.* *Your policy should set out criteria and the procedures for responding to applications for access to PHI you hold. It applies to individuals making application for their own PHI and to persons authorized to act on behalf of another individual (e.g. a parent, legal guardian, substitute decision-maker or lawyer).* *Your written procedures for managing access/correction requests should include:* • *statutory timelines for responding to access requests;* • *time extensions;* • *contents of the response;* • *how access is to be granted;* • *refusing access;* • *fees;* • *notifying applicants if their PHI is in the custody or control of another custodian; and* • *managing requests for correction of an individual's PHI.*

Appendix B – Sample public statement of information practices (s. 21)

Disclaimer to custodians: This is a sample only. It may not be suitable for your circumstances and should not be relied on as legal advice.

Statement of information practices – *sample*

Name of business	Address
Telephone	Email address

This document outlines how we protect the personal health information we collect about you. Personal health information (PHI) is any identifying information about you, including your physical and mental health. We value patient privacy and are committed to being accountable for how we treat your personal health information. Everyone working for this office is required to adhere to our privacy policies and procedures.

Our privacy policies and procedures were developed in compliance with the Yukon *Health Information Privacy and Management Act* (HIPMA). HIPMA sets out rules for how health care organizations, such as our office, can collect, use, disclose, and manage your PHI. If you have any questions regarding our privacy practices, please contact **<insert name of contact individual>.**

Collection, use and disclosure of personal health information

What personal health information do we collect?

We collect the following personal health information:

- identification and contact information (name, address, date of birth, telephone number, emergency contact, etc.);
- billing information (territorial/provincial plan and/or private insurer); and
- health information (symptoms, diagnosis, medical history, test results, reports and treatment, record of allergies, prescriptions, etc.)

Why do we collect your personal health information?

We collect your personal health information for the purpose of identifying you, providing you with health care, administering the services that we provide and communicating with you. We collect only the information that is required to fulfill those purposes. We do not collect any other information, or allow information to be used for other purposes, without your consent, except where authorized to do so, by law.

Consent for the collection, use, and disclosure of personal health information

Consent for provision of health care:

We only collect, use and disclose your PHI with your consent. We obtain your consent by providing you with a notice that describes the PHI we collect, how we use it and to whom we disclose this information. If we collect, use, or disclose your PHI other than as described in the notice, we will seek your consent unless we are authorized or required by law to collect, use, or disclose your PHI. A copy of our notice can be viewed by clicking on this link <insert link to notice>.

When and to whom do we disclose personal health information (PHI)?

Disclosure to other health care providers:

As specified in the notice, we may disclose your PHI to other health care providers who are involved in your care, including (but not limited to) other physicians and specialists, pharmacists, lab technicians, nutritionists, physiotherapists and occupational therapists. While your consent is implied through the notice, generally the disclosure of your PHI will include a discussion with your health care provider ahead of time, for example where a referral to a specialist is necessary. This ensures you remain informed of what information is being disclosed and allows you to make informed decisions about your health care. We also disclose your PHI to insured health providers for billing purposes.

Disclosures authorized by law:

There are limited situations where we are legally required to disclose your PHI without your consent. These situations include (but are not limited to) reporting infectious diseases, concerns about your ability to operate a motor vehicle, or by court order.

Disclosures to all other parties:

We will obtain your consent before disclosing your PHI to third parties for any purpose not specified in the notice unless we are authorized to do so by law. We will obtain your express consent if we collect, use or disclose your PHI for any fundraising activities, research or marketing, or if the disclosure is to public media.

Withdrawal of consent:

At any time, you can withdraw your consent for the collection, use, or disclosure of your PHI for any purpose, except when it is required by law or by established standards of professional practice. To withdraw your consent, you must do so in writing and provide the written withdrawal to your health care provider. Prior to withdrawing consent, we encourage you to

discuss the matter with your health care provider first so they can explain the possible consequences of withdrawing consent.

Patient rights

How can records be accessed?

You have the right to access any records containing your own PHI in a timely manner. You may request a copy of your records. If you wish to view an original record, one of our staff must be present to maintain the integrity of the record. Please note that in some circumstances, there may be a fee for accessing your records. Requests for access to your records can be made in writing and sent to **<insert contact individual's name and contact information>**. You do **not** have the right to access any other person's PHI unless you have their express consent to do so or if you have been designated as a substitute decision maker for the individual that the information is about.

Are there limitations on access?

In rare circumstances you may be denied access to your records, for example if providing access would create a significant risk to you or to another person.

What if the records are not accurate?

We make every effort to ensure that your information is recorded accurately. If an inaccuracy is identified, you can request that the information be corrected, and a note will be made to reflect this on your file. Please note that correction of your PHI is limited to factual information and does not apply to a health care provider's professional opinion or observation.

Office safeguards

How do we secure your personal information?

Safeguards are in place to protect your PHI. These safeguards include a combination of physical, technical and administrative security measures that are appropriate to the sensitivity of the information. These safeguards are aimed at protecting your PHI against loss or theft, as well as unauthorized access, disclosure, copying, use or modification. If there is a breach of your PHI that creates a risk of significant harm to you, you will be notified.

How do we communicate with you?

We protect PHI regardless of the format. Specific procedures and safeguards are in place for ensuring that communications by phone, email, fax, and post/courier remain secure. This includes authentication procedures and a secure file transfer platform.

How long do we keep your PHI?

We retain patient records for a minimum period of **<insert>** years, or as otherwise required by law and professional regulations.

How do we dispose of your PHI when it is no longer required?

When information is no longer required, it is destroyed in an irreversible and secure manner.

Questions, comments or complaints?

If you have any questions, comments or would like to file a complaint regarding our office's compliance with this statement of practice or with HIPMA, please first contact us directly to discuss your concerns.

<Name of your contact individual>

<Contact information>

You may also choose to make a complaint to the following:

Yukon Information and Privacy Commissioner
3162 Third Avenue
Whitehorse, Yukon Y1A 1G3
867 667 8468 or toll free in Yukon 1 844 997 8468
YukonIPC.ca
info@yukonaccountability.ca

Please do not email PHI to our office because it is not a secure form of communication.

Appendix C – Sample consent notice

Disclaimer to custodians: This is a sample only. It may not be suitable for your circumstances and should not be relied on as legal advice.

Instructions: *Under HIPMA, custodians may rely on a notice for obtaining knowledgeable consent to collect, use, or disclose an individual's personal health information (PHI). Refer here for more information about your privacy notice requirements.*

Personal health information (PHI) and your privacy

Yukon's *Health Information Privacy and Management Act* (HIPMA) protects the privacy of your PHI. As a custodian, we are responsible for collecting, using, disclosing and protecting your PHI in accordance with HIPMA.

Consent

We are authorized to collect, use, and disclose PHI about you with your consent and this notice sets out why we do this.

Please read this notice carefully as it is through this notice that you provide us with your consent to collect, use and disclose your personal health information.

What PHI we collect, use, and why

We collect and use your personal health information:

- to provide you with health care; and
- to arrange for payments related to your health care.

We will collect your name, contact information, and any other relevant information that is necessary to provide you with health care.

We will also collect your health care insurance number and any other information that is necessary to facilitate payment for your health care.

We only collect the minimal amount of PHI that is necessary.

What PHI we disclose and why

We only disclose your PHI to:

- care providers outside our organization if your PHI is required to provide you with care; and
- health care insurance plan providers to receive payment for your health care.

We will only disclose the minimal amount of your personal health information that is necessary.

Appendix C – Sample consent notice

You may refuse or withdraw your consent at any time

If you do not want your PHI collected, used, or disclosed for any or all the purposes described above, you may refuse your consent.

If you give consent and change your mind, you may withdraw your consent. To do so, you must provide your withdrawal in writing and provide it to **<insert contact name>.**

You should discuss any refusal or withdrawal of your consent with your health care provider before exercising this right, so that any consequences can be explained to you.

There are circumstances where your consent is not required

We will only collect, use, or disclose your PHI without your consent if we are authorized or required by HIPMA and its regulations. We are required to disclose infectious disease information about you to a public health officer or if we are ordered by a court.

Information disclosed outside Yukon will be governed by other laws

If we are authorized to disclose your PHI outside of the Yukon, the laws of that location will apply to the collection, use or disclosure of your PHI.

We can answer your questions

If you wish to ask your health care provider about the collection, use, or disclosure of your PHI, we will answer any questions you have so that you can exercise your right to refuse or withdraw consent.

Your concerns will be addressed

If you have any concerns about our collection, use, disclosure, and protection of your PHI, please contact any of our staff or our privacy officer, **<insert contact information>.**

You may also contact the Yukon Information and Privacy Commissioner.

3162 Third Avenue
Whitehorse, Yukon Y1A 1G3
867 667 8468 or toll free in Yukon 1 844 997 8468
YukonIPC.ca

Appendix D – Additional resources

Resources from the Information and Privacy Commissioner

These resources can be found at YukonIPC.ca/resources.

HIPMA Audit tool

Resources for custodians

- Guidance documents
- Frequently asked questions
- Information sheets

Resources from the Department of Health and Social Services

- HIPMA online training course
- HIPMA materials to post for the public
- Sample policies and forms

Resources from the Office of the Privacy Commissioner of Canada