Readiness Checklist for Custodians

Note: This checklist is meant to assist custodians by identifying key actions they can take as part of their assessment of and preparations for HIPMA compliance. It is a general guide only that may not be suitable for your circumstances and should not be relied on as legal advice.

Preparing for Yukon's *Health Information Privacy and Management Act* (*HIPMA*)

1. *HIPMA* Contact Person

☐ Have you chosen one or more individuals to act as your *HIPMA* contact person and provided them with the necessary training to fulfill the role? This individual (s) must:

- ➞ receive and process public complaints about your information practices, as well as help individuals in making complaints about your organization, including complaints to the IPC
- ➞ respond to access requests for records containing an individual's personal health information (PHI) and requests to correct PHI in the records
- ➞ educate and train employees and other agents (e.g., 3rd party contractors, volunteers) about their *HIPMA* responsibilities and your organization's practices
- ➞ respond to the individuals affected by a security breach and the IPC, where notification of a security breach is required (Refer to Section 30 of *HIPMA*)
- ➞ facilitate your organization's compliance with *HIPMA*

Actions Required/Notes:

_____

_____

_____

_____

2. Privacy and Security Training and Awareness

☐ Do you have a plan to train staff and other agents on privacy and security at orientation and on an ongoing basis? Does training occur before new staff and agents are granted access to PHI?

☐ Have you trained your current staff and other agents on *HIPMA* and your organization's privacy policies, so they are prepared for when the law comes into force?

☐ Have you developed a way for documenting when staff and other agents have completed their training and how to retain this documentation?

☐ Have you considered other means to raise privacy awareness in your organization, e.g. staff meetings focused on privacy, case studies, posters, FAQs, etc?

Related Toolkit Documents: *HIPMA* Online training course, (also available as adaptable PowerPoint slides), *HIPMA* FAQs for Staff and other Agents.

Actions Required/Notes:

3. Confidentiality Agreements

☐ Have your staff and other agents signed a confidentiality agreement with your organization that includes an acknowledgement that they are bound by *HIPMA* and information about the consequences of breaching the *Act*?

☐ Do you have a plan to have agents reaffirm their confidentiality agreement on a regular basis and to store these confidentiality agreements in case they are needed in the future?

Related Toolkit Documents: Sample Pledge of Confidentiality

Actions Required/Notes:

4. Written Statement of Information Practices for the public

☐ Have you developed a written document that provides the public with the following information:

- ➞ a general description of your organization's information practices
- ➞ how an individual can reach your contact person
- ➞ how individuals can request a record of their PHI or corrections to a record that you are the custodian of
- ➞ how to make a complaint to your organization and the IPC

☐ How have you made this document available to the public (e.g. website, printed brochure in your office)?

☐ Are your staff familiar with the contents of the document?

Related Toolkit Documents: Sample *HIPMA* brochure/handout

Actions Required/Notes:

Readiness Checklist for Custodians

5. Privacy Complaints and Security Breaches

☐ Have you established an effective procedure for receiving and responding to complaints regarding your information practices?

☐ Do you have a written breach policy that describes how to identify, report, manage, and learn from breaches? Does it make clear that your staff and other agents are required by law to report breaches involving PHI they handle to you at the first reasonable opportunity?

☐ Do you have a process for determining when an individual and the IPC must be informed of a breach and for notifying them in the manner required by *HIPMA* (e.g. the notice must include a description of the breach circumstances and PHI involved, when it happened, measures taken to reduce the risk of harm to the individual and the name of your HIPMA contact.)?

☐ Do you maintain a written record of all your breaches, so that trends can be identified and measures undertaken to minimize the risk of future breaches.

Related Toolkit Documents: Sample Breach Policy and Sample Breach Reporting Form.

Actions Required/Notes:

6. Access and Correction Requests from Individuals regarding their record

☐ Do you have a written policy that describes how your organization grants access to records under *HIPMA* and its regulations, including how to make a request, how fees will apply, timelines for your response, and situations where partial access or no access may be granted?

☐ Do you have a procedure for responding to correction requests from an individual, including a process to make changes to a written or electronic record of PHI or add a statement of disagreement where required?

Related Toolkit Documents: Sample Access to PHI Policy and Sample Application for Access to PHI Form

Actions Required/Notes:

7. Record of User Activity Requests from Individuals

☐ Have you identified any and all electronic information systems that maintain PHI you are the custodian of?

☐ Have you identified which of these systems have the ability to produce a record of user activity in accordance with *HIPMA* (i.e. the system has the ability to generate a report that identifies, for each time a user accesses PHI in the system, the identity of the user, the date and time of the access, and a description of what PHI is or could have been accessed)? Do you have a plan for creating this functionality in EIS that currently lack it?

☐ Do you have a process for receiving and responding to requests that includes the requirement that fees cannot be charged for a record of user activity?

☐ Do you have a retention schedule for these records?

Related Toolkit Documents: Sample Record of User Activity Request Form and Step-by-Step Guide to Complete the Record of User Activity Form

Actions Required/Notes:

8. Information Manager Agreements

☐ Have you identified any and all "information managers" (e.g. paper shredding services, IT service providers) engaged by your organization?

☐ Do you have written agreements with all information managers that contain the requirements of *HIPMA* and its regulations, including clauses that specify:

- ➞ the objectives of the agreement and guiding principles
- ➞ control of PHI is retained by the custodian, who must be allowed to access or obtain PHI
- ➞ what PHI the information manager can collect, use and disclose
- ➞ the purposes the information manager can collect, use and disclose PHI, and any limitations or conditions
- ➞ the custodian must be immediately forwarded all access and correction requests, as well as promptly advised, of all warrants, summons, court orders, etc., that the information manager receives
- ➞ the information manager must have safeguards that meet or exceed *HIPMA* requirements
- ➞ subcontracting is only allowed with the custodian's consent
- ➞ the custodian is allowed to verify and monitor the information manager's compliance with the agreement
- ➞ the information manager will notify the custodian at the first reasonable opportunity of any breach of the agreement and the custodian may terminate the agreement because of a breach
- ➞ if the agreement is terminated, the transfer of PHI by the information manager must be done in a manner that is cooperative and allows for ongoing access to the information. Once the transfer is complete, the information manager must securely destroy all records of the PHI

☐ Do you have a process for retaining these agreements?

Actions Required/Notes:

9. Information Practices

Custodians must have in place reasonable measures that will protect the confidentiality, privacy, security and integrity of PHI in their custody and control and prevent security breaches. A number of information practices are required under *HIPMA* and its regulations. While *HIPMA* does not explicitly state custodians must have an inventory of all their PHI holdings, it can assist custodians in ensuring they have the required information practices in place.

☐ Do you have in place administrative policies, (e.g. privacy policy, security policy, user access policy, breach policy or a clean desk policy) to protect personal health information? Certain policies, such as your access to records, privacy breach, and collection, use and disclosure of PHI policies, must be in writing.

☐ Do you have in place reasonable physical safeguards, such as locked cabinets or key card controlled access to areas where PHI is stored? Do you maintain PHI in designated areas and have in place security measures to protect it, including limiting physical access to authorized persons?

☐ Have you implemented reasonable technical safeguards, such as encryption of laptops and other mobile devices that store PHI, strong passwords, anti-virus protection and firewalls?

☐ Do you have policies or procedures in place for the secure storage, disposal (e.g. PHI is not disposed of in regular garbage) and destruction of PHI (e.g. hard drives are wiped before computers are sold for salvage) in your custody or control?

☐ Do you have a policy describing how long you retain PHI, including PHI contained in both paper and electronic formats?

☐ Do you have policies and procedures that address user access management and associated controls, including determining what access an agent needs based on their role (e.g. developing role based user access matrix for an electronic information system) and implementing controls that verify the user's identity and limits user access to what is needed (e.g. instead of having an electronic shared folder containing PHI accessible to everyone, restrict access to only those who need it and have some means of authenticating users with access to the file).

☐ Do you have policies and procedures that address the privacy and security risk of removable media and remote access to your information systems where applicable, including via an agent's own personal electronic communication device?

☐ Do you have a plan for how you will conduct an audit of your security safeguards, including your information practices and procedures, at least every two years? Deficiencies identified in an audit must be addressed as soon as possible.

Actions Required/Notes:

10. Consent Management

This section addresses your organization's consent model. In certain circumstances, *HIPMA* requires express consent or no consent, e.g. mandatory disclosures of PHI, in relation to the collection, use and disclosure of PHI. In other circumstances, you can determine whether you will rely on express consent, implied consent or no consent, where permitted under the *Act*, to collect, use and disclose PHI.

A. Elements of Consent

☐ Do you obtain consent from the individual for the collection, use or disclosure of personal health information, unless you are required or permitted to do otherwise by *HIPMA* or other law?

☐ Is consent knowledgeable? (For consent to be considered knowledgeable, individuals must know the purpose of the collection, use or disclosure of their personal health information, that they can give, withhold or withdraw their consent, and without their consent, their PHI can only be collected, used and disclosed as per *HIPMA* and its regulations). See the Notice of Purposes section below for when you can assume consent is knowledgeable.

☐ Is the consent related to the PHI being collected, used or disclosed and the associated purpose?

☐ Is the consent voluntary (consent cannot be obtained by fraud, misrepresentation or coercion)?

B. Notice of Purposes

Under *HIPMA*, a custodian can assume that an individual's consent is knowledgeable in regards to the collection, use or disclosure of the individual's PHI if a notice that meets the requirements of the *Act* is made readily available. This assumption cannot be made if there are reasonable grounds to believe the individual cannot read or has an impaired ability to understand the information or the language the notice is written in.

☐ Have you developed a written document that provides the public with the following information:

- ➞ the purposes for which you collect, use and disclose personal health information
- ➞ that an individual may withhold or withdraw their consent to the collection, use and disclosure of their PHI for the purpose of providing health care to them
- ➞ that without their consent, their PHI can only be collected, used and disclosed as permitted by *HIPMA* and its regulations
- ➞ that if PHI is disclosed outside Yukon, the law of that jurisdiction will apply to its collection, use and disclosure in that jurisdiction
- ➞ a general description of your record retention schedule

- ☐ Is the document written using plain language?
- ☐ Is the document available in either French or English? It may also be made available in other languages.
- ☐ How have you made this document readily available to the public? Is it posted in your registration/admission/waiting/entrance areas? Is it available on a website or part of an admission package?
- ☐ Are the appropriate staff familiar with the contents of the document and able to explain the document to those who may not understand it or who have basic questions?

Related Toolkit Documents: Sample Privacy Notice/Poster

Actions Required/Notes:

_____

_____

_____

_____

C. Express Consent

- ☐ Where applicable, do you obtain express consent for the collection, use and disclosure of personal health information? Express consent is required for the following purposes: fundraising activities, media, marketing and research (some exceptions apply for research, e.g. section 67 of *HIPMA*)
- ☐ Do you record all instances of express consent? Express consent can be given verbally as well as in writing, but all instances of express consent must be documented.
- ☐ Have the elements of consent been met?

D. Implied Consent

- ☐ Where applicable, do you rely on implied consent for the collection, use and disclosure of personal health information? For example, implied consent is the consent standard for the collection and use of personal health information for the provision of health care. The *Act* permits implied consent to be used as the standard for consent, unless express consent is required.
- ☐ Have the elements of consent been met?

E. Consent not required

- ☐ If you will collect, use or disclose personal health information without consent, has your authority under the *Act* to do so been documented and confirmed?
- ☐ Do you have a process in place to ensure there is a record of personal health information (with exception of registration and provider registry information) disclosed without consent, as required by section 22 of *HIPMA*?

F. Withdrawal, Refusal or Conditional Consent (sometimes referred to as "Consent Directives")

☐ Where consent has been obtained, are there procedures in place to address an individual's request to withdraw or to limit his or her consent to the collection, use and disclosure of PHI?

☐ Do the procedures include the requirement that requests must be submitted in writing to the custodian or their agent, address situations where requests don't apply or can be refused, and incorporate the custodian's legal duties when a request relates to the provision of healthcare (e.g. if a request is refused in relation to the provision of healthcare, the individual must be told of the decision as soon as reasonably possible and informed of their right to complain to the IPC). (See sections 36, 42–44 of *HIPMA*)

G. Capacity and Substitute Decision Makers (Sections 45–47 of *HIPMA*)

☐ Do you have procedures for determining the capacity of an individual to consent to the collection, use and disclosure of PHI?

☐ Do you have a process in place to ensure that where the individual lacks capacity, the appropriate substitute decision maker is determined in accordance with *HIPMA*?

☐ Where a person is deceased, is there a process recognizing that the deceased's personal representative can exercise the individual's rights under *HIPMA* when it relates to the administration of the deceased's estate or a claim made under an insurance policy for benefits payable upon death?

Actions Required/Notes:

11. Collection, Use and Disclosure of PHI

A. General Requirements

☐ Do you have written policies that describe how and why your organization collects, uses and disclosures personal health information and are they compliant with *HIPMA* and its regulations? (custodians can only collect, use, disclose and access PHI in accordance with *HIPMA* and its regulations, subject to limited legal exceptions)

☐ Do you use or disclose other data, or de-identify personal health information, when it will serve the purpose rather than use or disclose PHI?

☐ Do you takes steps to limit the personal health information that is collected, used or disclosed to only what PHI is necessary to achieve the purpose of the collection, use and disclosure?

Readiness Checklist for Custodians

B. Manner of collection

☐ Do you only collect personal health information directly from the individual about whom the information pertains?

☐ If you collect personal health information about an individual indirectly from other sources, do you have the individual's consent or does the collection fall under one of the exceptions specified in section 54 of *HIPMA*?

☐ Do you have policies or procedures in place that demonstrate the reasonable efforts your organization makes to ensure PHI collected from the individual or another source is accurate?

C. Use and Disclosure

☐ If you do not obtain consent from the individual for every use of their personal health information, does the use meet one of the criteria outlined in section 56 of the *Act*?

☐ If you do not have consent to disclose an individual's personal health information, is the reason for the disclosure one of the circumstances contemplated under sections 58–64 of *HIPMA* and its regulations?

☐ If you are a custodian who runs a hospital or a health facility, are you and your staff aware of section 59 of the *Act*, which describes when and what PHI you can disclose about an individual to immediate family or close personal friends without having obtained the individual's consent.

☐ Does your organization's written disclosure policy address when and how PHI can be disclosed without consent to third parties, e.g. law enforcement officers, professional regulatory bodies, etc.

☐ Do you have procedures in place for determining when you may need to disclose an individual's PHI to others without their consent in order to ensure they receive timely follow up care, in accordance with section 62 of *HIPMA*?

D. Collection, use and disclosure of the Yukon Health Care Insurance Plan (YCHIP) card and Yukon public health insurance plan number

☐ As a custodian, do you request the YHCIP card and collect, use or disclose the plan number for a purpose related to the provision of publically funding healthcare to the individual?

☐ If you request the card or collect, use or disclose the plan number for other purposes, is it related to one of the following approved purposes under *HIPMA* and its regulations:

- ➞ life, health or disability insurance claims
- ➞ health research
- ➞ *Workers' Compensation Act*, the *Jury Act*, the *Coroners Act* or the *Occupational Health and Safety Act*
- ➞ a proceeding
- ➞ Canadian Institute for Health Information (CIHI) agreements
- ➞ Yukon Health Information Network (YHIN)

E. Collection, use and disclosure of PHI for health research

☐ If you collect PHI for research, have you obtained prior approval for the collection from an institutional research review committee, unless an exemption applies (see section 66 of *HIPMA*)?

☐ Do you have in place policies or procedures that require an individual's consent to be obtained before releasing PHI to a researcher, where the research requires direct contact with the individual?

☐ If the proposed research meets the criteria in section 68 of *HIPMA* and it appears that PHI can be disclosed to a researcher without the individual's consent, do you have a process in place for verifying the research has been approved by an institutional review committee and there is an agreement in place between you as the custodian and the researcher that meets the requirements of section 69 of *HIPMA* and the regulations, before you disclose the PHI to the researcher?

Related Toolkit Documents: Sample Collection of PHI, Use of PHI and Disclosure of PHI policies

Actions Required/Notes: