Yukon Information and Privacy Commissioner

Health Information Privacy and Management Act (HIPMA)

What Custodians Need to Know About Their Responsibilities

About this Document

This document was created by the Office of the Information and Privacy Commissioner (IPC) to help custodians learn about their responsibilities under HIPMA. The document highlights some responsibilities that custodians will be required to manage daily and references the applicable sections in HIPMA for ease of cross reference. This document is intended to be used as an educational tool only. It does not contain all the requirements that a custodian must follow in HIPMA. It is up to each custodian to understand their obligations in HIPMA and to comply with them.

BASIC INFORMATION
HIPMA is a complete governance scheme for the collection, use, disclosure and management of personal health information (PHI). You cannot collect, use or disclose PHI unless HIPMA permits it.
There are two foundational rules in HIPMA that you must follow for *every* collection, use or disclosure of PHI (s.15-16). You must not collect, use or disclose PHI if other information will suffice. And, if HIPMA permits you to collect, use or disclose PHI, you must only collect, use or disclose the minimum amount that is reasonably necessary.
CONSENT
You can rely on implied consent to collect, use or disclose PHI (s.33). There are a few exceptions to this where express consent is required (s.34 and s.19 of the Regulation).
To rely on implied consent, the consent must be knowledgeable, relate to the PHI, be given voluntarily and obtained lawfully (s.38). The rules about obtaining consent are in s.32 to 47.
COLLECTION
There are only 3 circumstances that authorize you to collect PHI (s.53). With the consent of the individual and for a lawful purpose. If the collection is authorized by law. And, if you are collecting PHI that is necessary to carry out a program or activity of a public body or a health care program or activity of a First Nation custodian.
You must collect PHI directly from an individual unless HIPMA authorizes indirect collection (s.54). You may indirectly collect PHI with the consent of the individual (ss.54(a)). See ss.54(b) and (c) for additional circumstances that authorize indirect collection without consent.
USE
You can only use PHI that is in your custody or control to provide health care or for another lawful purpose if you have consent. You must stop using it at the individual's direction (ss.55(1)). The direction must be in the form of an express refusal or a withdrawing of consent to that use (p.55(1)(a) and s.20 of the Regulation).
There are a limited number of circumstances that allow you to use PHI without consent (s.56). See s.56 for a list of uses authorized without consent.
DISCLOSURE
You can disclose an individual's PHI to the individual or, with their consent, to another person (s.57).
There are a limited number of circumstances that allow you to disclose an individual's PHI without their consent (s.58). See s.58 for a list of disclosures authorized without consent. If you disclose PHI without the consent of the individual you must record about the disclosure. See ss.22(1) for what must be recorded.

If certain preconditions are met, and you don't think it will cause harm, you can disclose defined and limited PHI of a person residing in a health facility without their consent to their family member or to a person with whom they have a close personal relationship (s.59). 'Health facility' is defined in the definitions (ss.2(1)). See ss.59(1) for the preconditions and s.59(2) for the specific PHI you are authorized to disclose.
ACCESS and CORRECTION
Individuals have a *right* under HIPMA to access their own PHI subject to certain limited and specific exceptions. You must respond to their request within 30 days or an additional 60 if more time is needed (s.24 to 27). If you don't, you will be deemed to have refused access. There are specific steps you are required to take to process an access request (s.26) and you may charge the prescribed fee (ss.24(2) and s.27 to 32 of the Regulation).
Individuals can request a correction to their PHI and you must respond to this request within 30 days, or 45 if additional time is needed (s.28). There are limitations on correction and steps you must take in managing a correction request. See s.28.
INFORMATION PRACTICES
You must have information practices to protect PHI that align with the requirements in HIPMA and you must make public a statement about your information practices (s.21). What these must at minimum entail are listed in s.19(2) and (3) and s.14 of the Regulation.
Any electronic system you use for processing PHI must be able to log any access to PHI in the system by any person with access (s.22(3)). Individuals have a *right* to access this log and you cannot charge a fee for providing access (s.24(3) and s.31 of the Regulation).
You are accountable for any records containing PHI in your custody and control until you transfer them as required by HIPMA (s.23). There are penalties that apply for failing to follow this rule. See s.23.
You are accountable to 'take reasonable measures' to ensure your employees or other agents comply with the HIPMA and regulations (s.49). 'Reasonable measures' is not defined.
If you use a third party or 'information manager' to manage your PHI, including electronic, you must enter into an agreement to manage that information (s.51). 'Information manager' is defined in the definitions (s.2). What an information management agreement must contain is in s.21 of the Regulation.
CONTACT INDIVIDUAL
You must designate a 'contact individual' to manage your obligations under HIPMA, including responding to complaints and access requests. If you don't, you will be the contact individual by default (s.20). The duties of a contact individual are contained in s.20(2).
SECURITY BREACH
You must notify affected individuals about a breach if there is a risk of significant harm to them. You must also notify the IPC about the breach at the same time (s.30). It is an offence not to notify if required to by HIPMA (sp.121(1)(g)(i)). You must determine if there is a risk of significant harm (ROSH) to an individual as result of the breach. If so, you must notify them about the breach. See ss.29(a) and s.30 for how to determine whether there is a ROSH and what the notice must contain.
You must provide the IPC with a report about the breach within a reasonable time after it occurs (s.31). See s.31 for what the report must contain.
MORE INFORMATION
You can get more information about your obligations under HIPMA by contacting the Office of the IPC. Hours are 8:30 AM and 4:30 PM, Monday to Friday, Phone: 1-867-667-8468 or toll free at 1-800-661-0408 ext. 8468.

This document is not intended, nor is it a substitute for legal advice. For the exact wording and interpretation of HIPMA, please read HIPMA in its entirety. This document is not binding on the Information and Privacy Commissioner.