Yukon Information and Privacy Commissioner

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

Health Information Privacy and Management Act

Audit Tool

General information	
Custodian name and address	
Privacy contact name	
Privacy contact phone number	
Date of audit	

This tool was developed by the Yukon Information and Privacy Commissioner to assist custodians in meeting the audit requirements of the *Health Information Privacy and Management Act* (HIPMA) and the *Health Information General Regulation* (Regulation). Please view the HIPMA and the Regulation for all the requirements that a custodian must follow in HIPMA. It is up to each custodian to understand their obligations in HIPMA and comply with them.

Security safeguards audit

Sections 19 of *Health Information Privacy and Management Act* (HIPMA) and section 14 of the *Health Information General Regulation* (Regulation) identify information management practices a custodian must have in place to be compliant with HIPMA.

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

HIPMA and the Regulation went into effect on August 31, 2016. Therefore, a custodian is required to conduct an audit of their security safeguards *at least* every two years afterward. The safeguards a custodian must have in place under HIPMA are the minimum required.

Security safeguards standard

Subsection 19 (1) of HIPMA and subsection 14 (2) of the Regulation require that the information practices referred to in section 19 of HIPMA be based on the standard of what is reasonable, considering the sensitivity of the personal health information. To clarify, reasonable relates to a standard that meets or exceeds the industry standards in a sector. Sensitivity presumes classification of information I in the custody of a custodian has taken place. For guidance on standards, see Appendix B.

About this tool

This tool is designed to help custodians identify whether they are meeting the minimum-security safeguard requirements in HIPMA. The tool contains worksheets identifying each safeguard that a custodian must have in place. There is space on each worksheet to record the policy, procedure, or practice adopted by the custodian to meet the requirement and, where applicable, to indicate whether the adopted safeguard meets the appropriate standard. There is also a table to identify risks and develop an action plan to address the risks including timelines.

The provisions referred to in the tool are set out in Appendix A. The remaining provisions, including definitions, are contained in HIPMA and the Regulation. Appendix B contains resources that may assist a custodian achieve compliance. This Appendix also contains best practices that may enhance a custodian's security safeguards beyond the minimum requirements.

Use of this tool is voluntary. There is no obligation for custodians to submit a completed copy of the tool to the Information and Privacy Commissioner's office (IPC). However, the IPC will accept submissions to be used for the sole purpose of identifying education and training needs, or other resources required by custodians to improve their information management practices.

The IPC has authority to investigate any complaint of non-compliance with HIPMA or the Regulation.[1] Therefore, custodians should retain a date-stamped and completed version of the audit tool (or other document if the tool is not used) along with any relevant attachments for a reasonable period of time as evidence it completed the audit as required by paragraph 14 (1)(c) of the Regulation. Note that it is an offence under HIPMA not to perform the audit.[2]

[1] See section 99 of HIPMA.

[2] See paragraph 121 (1)(b) of HIPMA.

Requirement: HIPMA paragraphs 19 (3)(h) plus paragraphs 14 (1)(c) and (d) of the Regulation

Does the custodian have a security safeguard audit policy or procedure?	Enter the answer below. If the custodian has implemented these policies as of the date of audit, they should be listed below and attached to this tool.
Does the custodian have a policy or procedure to address any deficiencies identified through its bi-yearly audit?	Enter the answer below. If the custodian has implemented these policies as of the date of audit, they should be listed below and attached to this tool.
Are these safeguards reasonable, taking into account the sensitivity of the personal health information?	Enter the answer below.
What, if any, are the gaps in these safeguards?	Enter the answer below. Elaborate below on how these gaps will be mitigated.

Gap	Mitigation action	Mitigation timeline
		____/____/____
		____/____/____
		____/____/____
		____/____/____
		____/____/____

Requirement: *HIPMA* paragraph 19 (3)(h) plus subparagraph 14 (1)(b)(i) of the Regulation

Does the custodian have written policies in relation to the collection, use and disclosure of PHI?	Enter the answer below. If the custodian has implemented these policies as of the date of audit, they should be listed below and attached to this tool.
Are these safeguards reasonable, taking into account the sensitivity of the personal health information?	Answer:
What, if any, are the gaps in these safeguards?	Answer: Elaborate below on how these gaps will be mitigated.

Gap	Mitigation action	Mitigation timeline
		____/____/____
		____/____/____
		____/____/____
		____/____/____
		____/____/____

Requirement: *HIPMA* paragraph 19 (3)(h) together with paragraph 14 (1)(b)(ii) of the Regulation

Does the custodian have a written policy on security breaches that describes how the custodian complies with Division 5 of Part 3 of the Act?	Enter the answer below. If the custodian has implemented these policies as of the date of audit, they should be listed below and attached to this tool.
Are these safeguards reasonable, taking into account the sensitivity of the personal health information?	Answer:
What, if any, are the gaps in these safeguards?	Answer: Elaborate below on how these gaps will be mitigated.

Gap	Mitigation action	Mitigation timeline
		____/____/____
		____/____/____
		____/____/____
		____/____/____
		____/____/____

Requirement: *HIPMA* paragraph 19 (3)(h) together with subparagraph 14 (1)(b)(iii) of the Regulation

Does the custodian have a written policy in relation to individuals' access to and correction of their personal health information?	Enter the answer below. If the custodian has implemented these policies as of the date of audit, they should be listed below and attached to this tool.
Are these safeguards reasonable, taking into account the sensitivity of the personal health information?	Answer:
What, if any, are the gaps in these safeguards?	Answer: Elaborate below on how these gaps will be mitigated.

Gap	Mitigation action	Mitigation timeline
		____/____/____
		____/____/____
		____/____/____
		____/____/____

Requirement: *HIPMA* paragraph 19 (3)(h) plus subsection 14 (1)(e) of the Regulation

Does the custodian have a policy or procedure to ensure	Enter answer below. If the custodian has implemented these policies as of the date of audit, they should be listed below and attached to this tool.

that removable media used to record, transport, or transfer personal health information are appropriately protected when in use and securely stored when not in use?	
Are these safeguards reasonable, taking into account the sensitivity of the personal health information?	Answer:
What, if any, are the gaps in these safeguards?	Answer: Elaborate below on how these gaps will be mitigated.

Gap	Mitigation action	Mitigation timeline
		____/____/____
		____/____/____
		____/____/____
		____/____/____
		____/____/____

Requirement: HIPMA paragraph 19 (3)(h) plus paragraph 14 (1)(h) of the Regulation

Does the custodian have a policy or procedure to ensure that a written record is	Enter the answer below. If the custodian has implemented these policies as of the date of audit, they should be listed below and attached to this tool.

created of all security breaches?	
Are these safeguards reasonable, taking into account the sensitivity of the personal health information?	Answer:
What, if any, are the gaps in these safeguards?	Answer: Elaborate below on how these gaps will be mitigated.

Gap	Mitigation action	Mitigation timeline
		____/____/____
		____/____/____
		____/____/____
		____/____/____
		____/____/____

Requirement: HIPMA paragraph 19 (3)(f)

Does the custodian have policies which provide that personal health information is retained in accordance with prescribed requirements?	Enter the answer below. If the custodian has implemented these policies as of the date of audit, they should be listed below and attached to this tool.
Are these safeguards reasonable, taking into account the sensitivity of the personal health information?	Answer:
What, if any, are the gaps in these safeguards?	Answer: Elaborate below on how these gaps will be mitigated.

Gap	Mitigation action	Mitigation timeline
		____/____/____
		____/____/____
		____/____/____
		____/____/____
		____/____/____

Requirement: HIPMA paragraph 19 (3)(g)

Does the custodian have procedures in place to receive and respond to complaints regarding its information practices?	Enter the answer below. If the custodian has implemented these policies as of the date of audit, they should be listed below and attached to this tool.
Are these safeguards reasonable, taking into account the sensitivity of the personal health information?	Answer:
What, if any, are the gaps in these safeguards?	Answer: Elaborate below on how these gaps will be mitigated.

Gap	Mitigation action	Mitigation timeline
		____/____/____
		____/____/____
		____/____/____
		____/____/____
		____/____/____

Requirement: *HIPMA* paragraph 19 (3)(h) plus paragraph 14 (1)(a)(i) of the Regulation

Has the custodian determined the personal health information that each of its agents are authorized to access?	Enter the answer below. If the custodian has implemented these policies as of the date of audit, they should be listed below and attached to this tool.
Are these safeguards reasonable, taking into account the sensitivity of the personal health information?	Answer:
What, if any, are the gaps in these safeguards?	Answer: Elaborate below on how these gaps will be mitigated.

Gap	Mitigation action	Mitigation timeline
		____/____/____
		____/____/____
		____/____/____
		____/____/____
		____/____/____

Requirement: *HIPMA* paragraph 19 (3)(h) plus subparagraph 14 (1)(a)(ii) of the Regulation

Have all agents of the custodian signed a pledge of confidentiality that includes an acknowledgement that the agent is bound by the Act and is aware of the consequences of breaching it?	Enter the answer to this question below and indicate how this is done. If the custodian has implemented these policies as of the date of audit, they should be listed below and attached to this tool:
Are these safeguards reasonable, taking into account the sensitivity of the personal health information?	Answer:
What, if any, are the gaps in these safeguards?	Answer: Elaborate below on how these gaps will be mitigated.

Gap	Mitigation action	Mitigation timeline
		____/____/____
		____/____/____
		____/____/____
		____/____/____
		____/____/____

Requirement: *HIPMA* paragraph 19 (3)(h) plus subparagraph 14 (1)(a)(iii) of the Regulation

Has the custodian provided privacy and security orientation and ongoing training for each of its agents?	Enter the answer below. If the custodian has implemented orientation and ongoing training as of the date of audit, associated material should be listed below and attached to this tool.
Are these safeguards reasonable, taking into account the sensitivity of the personal health information?	Answer:
What, if any, are the gaps in these safeguards?	Answer: Elaborate below on how these gaps will be mitigated.

Gap	Mitigation action	Mitigation timeline
		____/____/____
		____/____/____
		____/____/____
		____/____/____
		____/____/____

Requirement: *HIPMA* paragraph 19 (3)(h) plus paragraph 14 (1)(i) of the Regulation

Does the custodian address the privacy and security risks of an agent's remote access to the custodian's information system, including through the use of the agent's own mobile electronic communication device?	Enter the answer below. If the custodian has implemented measures to address these risks as of the date of audit, associated material should be listed below and attached to this tool.
Are these safeguards reasonable, taking into account the sensitivity of the personal health information?	Answer:
What, if any, are the gaps in these safeguards?	Answer: Elaborate below on how these gaps will be mitigated.

Gap	Mitigation action	Mitigation timeline
		____/____/____
		____/____/____
		____/____/____
		____/____/____
		____/____/____

Requirement: *HIPMA* paragraph 19 (3)(h) plus paragraph 14 (1)(g) of the Regulation

Does the custodian limit physical access to designated areas containing personal health information to authorized persons?	Enter the answer below. If the custodian has implemented measures to address these risks as of the date of audit, associated material should be listed below and attached to this tool.
Are these safeguards reasonable, taking into account the sensitivity of the personal health information?	Answer:
What, if any, are the gaps in these safeguards?	Answer: Elaborate below on how these gaps will be mitigated.

Gap	Mitigation action	Mitigation timeline
		____/____/____
		____/____/____
		____/____/____
		____/____/____
		____/____/____

Requirement: *HIPMA* paragraph 19 (3)(a)

Has the custodian implemented measures that protect the confidentiality, privacy, integrity, and security of personal health information and that prevent its unauthorized modification?	Enter the answer below. If the custodian has implemented measures to address these risks as of the date of audit, associated material should be listed below and attached to this tool.
Are these safeguards reasonable, taking into account the sensitivity of the personal health information?	Answer:
What, if any, are the gaps in these safeguards?	Answer: Elaborate below on how these gaps will be mitigated.

Gap	Mitigation action	Mitigation timeline
		____/____/____
		____/____/____
		____/____/____
		____/____/____
		____/____/____

Requirement: *HIPMA* paragraph 19 (3)(b)

Has the custodian implemented controls that limit the individuals who may use PHI to those specifically authorized by the custodian to do so?	Enter the answer below. If the custodian has implemented measures to address these risks as of the date of audit, associated material should be listed below and attached to this tool.
Are these safeguards reasonable, taking into account the sensitivity of the personal health information?	Answer:
What, if any, are the gaps in these safeguards?	Answer: Elaborate below on how these gaps will be mitigated.

Gap	Mitigation action	Mitigation timeline
		____/____/____
		____/____/____
		____/____/____
		____/____/____
		____/____/____

Requirement: *HIPMA* paragraph 19 (3)(c)

Has the custodian implemented controls to ensure that PHI cannot be used unless the identity of the individual seeking to use the PHI is verified as an individual the custodian has authorized to use it, and the proposed use is verified as authorized under this Act?	Enter the answer below. If the custodian has implemented measures to address these risks as of the date of audit, associated material should be listed below and attached to this tool.
Are these safeguards reasonable, taking into account the sensitivity of the personal health information?	Answer:
What, if any, are the gaps in these safeguards?	Answer: Elaborate below on how these gaps will be mitigated.

Gap	Mitigation action	Mitigation timeline
		____/____/____
		____/____/____
		____/____/____
		____/____/____
		____/____/____

Requirement: *HIPMA* paragraph 19 (3)(d)

Has the custodian taken all reasonable steps to prevent a security breach?	Enter the answer below. If the custodian has implemented measures to address these risks as of the date of audit, associated material should be listed below and attached to this tool.
Are these safeguards reasonable, taking into account the sensitivity of the personal health information?	Answer:
What, if any, are the gaps in these safeguards?	Answer: Elaborate below on how these gaps will be mitigated.

Gap	Mitigation action	Mitigation timeline
		____/____/____
		____/____/____
		____/____/____
		____/____/____
		____/____/____

Requirement: *HIPMA* paragraph 19 (3)(e)

Does the custodian provide for the secure storage, disposal and destruction of records?	Enter the answer below. If the custodian has implemented measures to meet this requirement as of the date of audit, associated material should be listed below and attached to this tool.
Are these safeguards reasonable, taking into account the sensitivity of the personal health information?	Answer:
What, if any, are the gaps in these safeguards?	Answer: Elaborate below on how these gaps will be mitigated.

Gap	Mitigation action	Mitigation timeline
		____/____/____
		____/____/____
		____/____/____
		____/____/____
		____/____/____

Requirement: *HIPMA* subsection 19 (1)

Has the custodian implemented 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?	Enter the answer below. **Note that the minimum information practices required under HIPMA are detailed in the preceding tables**. List all additional practices that are in place as of the date of audit and, where applicable, attach them to this tool.
Are these safeguards reasonable, taking into account the sensitivity of the personal health information?	Answer:
What, if any, are the gaps in these safeguards?	Answer: Elaborate below on how these gaps will be mitigated.

Gap	Mitigation action	Mitigation timeline
		____/____/____
		____/____/____
		____/____/____
		____/____/____
		____/____/____

Appendix A

Provisions of HIPMA and the Regulation

***Health Information Privacy and Management Act,* S.Y. 2013, c.16**

DIVISION 3 OF PART 3 – Information practices

Custodian's information practices generally

19(1) A custodian must protect personal health information 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.

(2) The information practices referred to in subsection (1) must be based on the standards that are prescribed for this purpose.

(3) Without limiting subsection (1), a custodian must, in relation to personal health information in its custody or control

(a) implement measures that protect the confidentiality, privacy, integrity and security of personal health information and that prevent its unauthorized modification;

(b) implement controls that limit the individuals who may use personal health information to those specifically authorized by the custodian to do so;

(c) implement controls to ensure that personal health information cannot be used unless

(i) the identity of the individual seeking to use the personal health information is verified as an individual the custodian has authorized to use it, and

(ii) the proposed use is authorized under this Act;

(d) take all reasonable steps to prevent a security breach;

(e) provide for the secure storage, disposal and destruction of records to minimize the risk of unauthorized access to, or disclosure of, personal health information;

(f) develop policies which provide that personal health information is retained in accordance with the prescribed requirements, if any;

(g) establish a procedure for receiving and responding to complaints regarding its information practices; and

(h) meet the prescribed requirements, if any. S.Y. 2013, c.16, s.19

DIVISION 5 OF PART 3 – Security breaches

Interpretation

29 For the purposes of this Division

(a) any event that it is reasonable to believe is a security breach in relation to personal health information in a custodian's custody or control is deemed to be a security breach in relation to that personal health information; and

(b) harm includes identity theft, identity fraud, damage to reputation and personal humiliation or embarrassment. S.Y. 2013, c.16, s.29

Notification of individual

30 (1) If a security breach occurs in relation to an individual's personal health information in a custodian's custody or control, and there are reasonable grounds to believe that the individual is at risk of significant harm as a result of the security breach, the custodian must, as soon as reasonably possible after the security breach, notify the individual of the security breach.

(2) Where subsection (1) requires a custodian to notify an individual of a security breach

(a) the custodian must, in the notice

(i) describe the circumstances of the security breach and the personal health information involved,

(ii) indicate when the security breach occurred,

(iii) describe the measures, if any, that the custodian has taken to reduce the risk of harm to the individual as a result of the security breach, and

(b) the custodian must at the same time give the commissioner a copy of the notice.

(3) In determining whether a custodian has reasonable grounds to believe that an individual is at risk of significant harm as a result of a security breach in relation to the individual's personal health information, the following are to be considered

(a) the length of time between the occurrence of the security breach and its discovery by the custodian;

(b) the likelihood that there has been any disclosure, unauthorized use or copying of the personal health information;

(c) the information available to the custodian regarding the individual's personal circumstances;

(d) the likelihood that the personal health information could be used for the purpose of identity theft or identity fraud;

(e) the number of other individuals whose personal health information is or may be similarly affected;

(f) the measures, if any, that the custodian took after the security breach to reduce the risk of harm to the individual as a result of the security breach; and

(g) any factor that is reasonably relevant in the circumstances or is prescribed for this purpose. S.Y. 2013, c.16, s.30

Report to commissioner

31 (1) If section 30 requires a custodian to notify an individual of a security breach in relation to the individual's personal health information in the custodian's custody or control, the custodian must, within a reasonable time after discovering the security breach, submit to the commissioner a written report that

(a) assesses the risk of harm to individuals as a result of the security breach, and estimates the number of individuals so affected; and

(b) describes the measures, if any, that the custodian has taken to reduce the risk of harm to individuals as a result of the security breach.

2) The commissioner may, after reviewing a report submitted by a custodian under subsection (1) in respect of a security breach, recommend to the custodian any measures that the commissioner considers appropriate to reduce the risk of similar breaches occurring in the future. S.Y. 2013, c.16, s.31

***Health Information General Regulation,* O.I.C. 2016/159**

Custodians' information practices

14(1) For the purposes of section 19 of the Act, a custodian must, in respect of personal health information that is in the custodian's custody or control

(a) for each of the custodian's agents

(i) determine the personal health information that the agent is authorized to access,

(ii) ensure that the agent signs a pledge of confidentiality that includes an acknowledgment that the agent is bound by the Act and is aware of the consequences of breaching it, and

(iii) where appropriate, provide privacy and security orientation and ongoing training;

(b) ensure that the custodian has, in writing

(i) policies in relation to the collection, use and disclosure of personal health information,

(ii) a policy on security breaches that describes how the custodian complies with Division 5 of Part 3 of the Act, and

(iii) a policy in relation to individuals' access to and correction of their personal health information;

(c) at least every two years, conduct an audit of the custodian's security safeguards, including their information practices and procedures;

(d) as soon as possible, identify and address any deficiencies identified in an audit conducted under paragraph (c);

(e) ensure that removable media used to record, transport or transfer personal health information are

(i) appropriately protected when in use, and

(ii) stored securely when not in use;

(f) ensure that personal health information is maintained in a designated area and is subject to appropriate security safeguards;

(g) limit physical access to designated areas containing personal health information to authorized persons;

(h) ensure that a written record is created of all security breaches; and

(i) address the privacy and security risks of an agent's remote access to the custodian's information system, including through the use of the agent's own mobile electronic communication device.

(2) The information practices referred to in section 19 of the Act (including, for greater certainty, those described in this section) must be based on the standard of what is reasonable, taking into account the sensitivity of the personal health information.

HIMPA resources

HIPMA guide for small custodians
Government of Yukon Health and Social Services

Other resources

Safeguards

Guidance on Safeguards (decisions of the Courts and Privacy Commissioner of Canada) for the *Personal Information Protection and Electronic Documents Act*

Retention and disposal

Personal Information Retention and Disposal: Principles and Best Practices, Office of the Privacy Commissioner of Canada 2014

Information security guidance for smaller organizations

Get Cyber Safe Guide for Small Businesses

Small Business Information Security: The Fundamentals, National Institute of Standards and Technology, U.S. Department of Commerce 2016

NIST Cybersecurity Framework 2.0 (Small Business Quick-Start Guide

Information security guidance for medium and large sized organizations

This International Standard provides guidance to healthcare organizations and other custodians of personal health information on how best to protect the confidentiality, integrity, and availability of such information. It is based upon and extends the general guidance provided by ISO/IEC 27002:2013 and addresses the special information security management needs of the health sector and its unique operating environments.

Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology 2018

Information security guidance for health care providers

Custodians may wish to check with their professional body or association at the local or national level. Some have guidance on best practices for securing personal health information. Below are some links to guidance available on the internet.

Canadian Medical Association, Policies and research, Policy documents, Health information and e-health

BC Physician Privacy Toolkit, A Guide for physicians in private practice, 3rd Ed.