Yukon
Information
and Privacy
Commissioner

3162 Third Avenue, Main Floor
Whitehorse, Yukon Y1A 1G3
T: 867.667.8468
Tollfree 1-800-661-0408 ext 8468
www.yukonombudsman.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 Office of the 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 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

Section 19 of the *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, taking into account 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 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 Office of the Information and Privacy Commissioner (OIPC). The OIPC will accept a copy. A copy received by the OIPC will be used solely for the purposes of identifying education and training needs, or other resources required by custodians to improve their information management practices.

The Information and Privacy Commissioner 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 (I){c) and (d) of the Regulation

Does the custodian have a security safeguard audit policy or procedure?	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.
Does the custodian have a policy or procedure to address any deficiencies identified through its bi-yearly audit?	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.
Are these safeguards reasonable, taking into account the sensitivity of the personal health information?	Enter answer below.
What, if any, are the gaps in these safeguards?	Enter answer below. Elaborate below on how these gaps will be mitigated.

Gap	Mitigation action	Mitigation timeline
		_ _j _ _J _
		_ _j _ _J _
		_ _j _ _J _
		_ _j _ _J _
		_ _j _ _J _

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

Does the custodian have written policies in relation to the collection, use and disclosure of PHI?	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.
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 gapswill be mitigated.

Gap	Mitigation action	Mitigation timeline
		_ _j _ _J _
		_ _j _ _J _
		_ _j _ _J _
		_ _j _ _J _
		_ _j _ _J _

Requirement: *HIPMA* paragraph 19 (3)(h} together with paragraph 14 (I)(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 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 (l)(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 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 (I)(e} of the Regulation

Does the custodian have a policy or procedure to ensure 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?	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.
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
		_ _j _ _J _
		_ _j _ _J _
		_ _j _ _J _
		_ _j _ _J _
		_ _j _ _J _

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

Does the custodian have a policy or procedure to ensure that a written record is created of all security breaches?	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.
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
		_ _j _ _J _
		_ _j _ _J _
		_ _j _ _J _
		_ _j _ _J _
		_ _j _ _J _

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 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 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 (I)(a)(i} of the Regulation

Has the custodian determined the personal health information that each of its agents are authorized to access?	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.
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 (I)(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
		_ _j _ _J _
		_ _j _ _J _
		_ _j _ _J _
		_ _j _ _J _
		_ _j _ _J _

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

Has the custodian provided privacy and security orientation and ongoing training for each of its agents?	Enter 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
		_ _j _ _J _
		_ _j _ _J _
		_ _j _ _J _
		_ _j _ _J _
		_ _j _ _J _

Requirement: *HIPMA* paragraph 19 (3)(h} plus paragraph 14 (I)(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 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
		_ _j _ _J _
		_ _j _ _J _
		_ _j _ _J _
		_ _j _ _J _
		_ _j _ _J _

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

Does the custodian limit physical access to designated areas containing personal health information to authorized persons?	Enter 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 gapswill be mitigated.

Gap	Mitigation action	Mitigation timeline
		_ _j _ _J _
		_ _j _ _J _
		_ _j _ _J _
		_ _j _ _J _
		_ _j _ _J _

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 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 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 gapswill be mitigated.

Gap	Mitigation action	Mitigation timeline
		_ _j _ _J _
		_ _j _ _J _
		_ _j _ _J _
		_ _j _ _J _
		_ _j _ _J _

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 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 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 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
		_ _j _ _J _
		_ _j _ _J _
		_ _j _ _J _
		_ _j _ _J _
		_ _j _ _J _

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 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 gapswill 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.

Appendix B

Resources on Best Practices for

Information Management and Security

HIPMA RESOURCES

- *What Custodians Need to Know About Their Responsibilities*, Yukon Information and Privacy Commissioner, 2016. **https://www.yukonombudsman.ca/uploads/media/57c5caaeba0a8/Final%20at-a-glance%20What%20Custodians%20Need%20to%20Know%20about%20their%20Responsibilities%20v%201%2016Aug26.pdf?v1**

- *HIPMA FAQs for Staff and other agents*, Yukon Health and Social Services 2016. **http://www.hss.gov.yk.ca/pdf/hipma_faq_for_staff_agents.pdf**

OTHER RESOURCES

Safeguards

- **Guidance on Safeguards (decisions of the Courts and Privacy Commissioner of Canada) for the *Personal Information Protection and Electronic Documents Act*** **https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_08_sg/**

Retention and Disposal

- *Personal Information Retention and Disposal: Principles and Best Practices*, Office of the Privacy Commissioner of Canada, 2014 **https://www.priv.gc.ca/en/privacy-topics/safeguarding-personal-information/gd_rd_201406/**

Information Security Guidance for Smaller Organizations

- *Cyber Security for Healthcare Organizations: Protecting Yourself Against Common Cyber Attacks*, Canadian Centre for Cyber Security, 2020. **https://cyber.gc.ca/en/guidance/cyber-security-healthcare-organizations-protecting-yourself-against-common-cyber-attacks**

- *Small Business Information Security: The Fundamentals*, National Institute of Standards and Technology, U.S. Department of Commerce, 2016. **https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.7621r1.pdf**

Information Security Guidance for Medium and Large Sized Organizations

- *ISO 27799:21016 Health informatics – information security management in health* https://www.iso.org/obp/ui/#iso:std:62777:en

Note - 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. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

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 *https://www.cma.ca/En/Pages/policies-research.aspx*

- *BC Physician Privacy Toolkit, A Guide for physicians in private practice, 3rd Ed.* https://www.doctorsofbc.ca/sites/default/files/ptv3.0.04.07_step_7_-_employ_safeguards.pdf

Appendix C
Recommended compliance check

Although not required as part of the audit. The requirements below are some important, but not all of, the mandatory requirements in HIPMA.

Continuing duties of custodian

Section 23 and 60 of HIPMA (below) set out the obligation for custodians to take care of the personal health information in their custody or control when they cease to operate in the Yukon (e.g., due to death or due to moving to another jurisdiction). This obligation includes the designation of and the transfer of records to a successor custodian.

The purpose of these provisions is to ensure that personal health information collected in the course of providing health care to an individual by a custodian is protected in accordance with HIPMA's rules until a custodian transfers the personal health information, that is in their custody or control, to a successor custodian who will take over the health care provided to the individual and who, upon transfer, will replace the original custodian in regard to the personal health information.

The notice requirement in subsection 60 (5) ensures that individuals are informed about what is happening with their personal health information and allows them to exercise control over records containing their personal health information by providing them the right to refuse the transfer of their records to a particular successor custodian.

The duties imposed under HIPMA on a custodian with respect to records containing personal health information apply to the custodian until the custodian transfers custody and control of the personal health information to the successor.

- **Ensure you designate a successor custodian.**
- **If you cease operations in the Yukon, ensure that the transfer of records happens in accordance with section 60 (e.g., providing notice of the transfer to the clients involved, see below for the full requirements).**

Sections 23 and 60 state the follows.

Continuing duties of custodian

23(1) The duties imposed under this Act on a custodian with respect to personal health information, and records containing personal health information, in the custody or control of the custodian apply to the custodian until the custodian transfers custody and control of the personal health information or the records to a successor of the custodian in accordance with section 60 or to a prescribed person in accordance with the prescribed requirements, if any.[1] [Emphasis added]

(2) If a custodian fails to carry out their duties under this Act, the Minister may, with the prior consent of the person to be appointed, appoint a person to carry out those duties in place of the custodian until custody and control of the personal health information or of the records are transferred to a successor of

[1] There is no prescribed person or requirements.

the custodian in accordance with section 60 or to a prescribed person in accordance with the prescribed requirements, if any.[2]

(3) An appointment under subsection (2) may be made subject to any terms and conditions that the Minister considers appropriate in the circumstances.

(4) The Minister may require a custodian who fails to carry out their duties under this Act

(a) to reimburse the Government of Yukon for any costs it reasonably incurs as a result of the custodian's failure; and

(b) to pay a person appointed under subsection (2) to carry out the custodian's duties an amount determined by the Minister, as compensation for the person's services under that subsection, and to reimburse the person for any disbursements it reasonably makes in providing the services.

60(1) In this section

"potential successor" of a particular custodian means a person who

(a) contemplates entering into an agreement with the particular custodian under which the particular custodian will relinquish to the person the custody and control of personal health information, and

(b) is a custodian or can reasonably be expected, if it enters into the agreement described in paragraph (a), to become a custodian;

"successor" of a particular custodian means another custodian to whom the particular custodian has, under an agreement between them, relinquished the custody and control of personal health information

(2) A custodian may, without an individual's consent, disclose the individual's personal health information to a potential successor of the custodian for the purpose of allowing the potential successor to assess and evaluate the operations of the custodian, if the potential successor first enters into an agreement with the custodian to keep the personal health information confidential and secure and not to retain it longer than is necessary for the purpose of the assessment or evaluation.

(3) A custodian may transfer a record of an individual's personal health information to the custodian's successor unless the individual expressly instructs the custodian not to make the transfer.

(4) If, under subsection (3), a custodian transfers a record of an individual's personal health information to the custodian's successor and an instruction of the individual prevents the custodian from transferring all the individual's personal health information that the custodian has reasonable grounds to believe is necessary for the provision of health care to the individual, the custodian must notify the successor of that fact.

(5) A custodian must make reasonable efforts to give notice to an individual before transferring a record of the individual's personal health information to the custodian's successor or, if that is not reasonably possible, as soon as possible after transferring the record. [Emphasis added]

[2] There are no prescribed requirements.

Requirement to Enter into an Information Management Agreement

Section 51 of HIPMA sets out the requirement for custodians to enter into an agreement with information managers.

HIPMA defines an information manager as follows;

"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;*

<u>Responsibilities of custodians and information managers</u>

Information managers of custodians have access to personal health information which is sensitive in nature. To ensure confidentiality of this information, the custodian must enter into an agreement with any information manager it uses. Section 51 of HIPMA and section 21 of the *Health Information General Regulation* (Regulation) set out the requirements for this agreement.

If an information manager has subcontractors, the terms of agreement with the information manager should include a requirement that the information manager will take all steps necessary to ensure their subcontractors will not cause them to violate the terms of their information management agreement with the custodian.

- **Ensure signed agreements are in place with all of the custodian's information managers and compliance by any of the information manager's subcontractors is accounted for.**
- **Ensure the agreement complies with the requirements as set out in section 51 of HIPMA and section 21 of the HIPMA general regulation.**

Section 51 of HIPMA and Section 21 of the Regulation state as follows.

Responsibilities of custodians and information managers

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

> *(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.*

(2) An information manager who enters into a written agreement under subsection (1) must

> *(a) comply with the duties imposed on the information manager under the agreement and the prescribed requirements, if any; and*

(b) notify the custodian at the first reasonable opportunity of any breach of the agreement by the information manager. S.Y. 2013, c.16, s.51

Regulation

21 When entering into a written agreement with an information manager in respect of personal health information under section 51 of the Act, a custodian must

(a) ensure that the agreement allows the custodian to maintain control of the personal health information; and

(b) ensure that the agreement contains provisions which;

(i) identify the objectives of the agreement and the principles that guide the agreement,

(ii) describe the types or classes of personal health information (referred to in this section as the "relevant personal health information") that the information manager may collect, use or disclose under the agreement, the purposes for which it may be collected, used or disclosed and any limitations or conditions on its collection, use or disclosure,

(iii) require the information manager

(A) to allow the custodian to access or otherwise obtain the relevant personal health information at any time, subject only to necessary operational constraints,

(B) to forward immediately to the custodian any access or correction request that is made in relation to the relevant personal health information,

(C) to maintain administrative, technical and physical safeguards that meet or exceed the safeguards required of the custodian under the Act to ensure the confidentiality, security and integrity of the relevant personal health information, and

(D) to inform the custodian promptly of the information manager's receipt of any requirement issued in a proceeding, including any summons, warrant or order, that relates to the relevant personal health information and that it is reasonable to believe may be enforceable in the jurisdiction in which the information manager operates or in which the relevant personal health information is located,

(iv) prohibit the information manager from subcontracting, without the custodian's written consent, any of the services to which the agreement relates,

(v) allow the custodian to monitor and verify compliance with the agreement by the information manager,

(vi) allow the custodian to terminate the agreement in the event of a breach of the agreement by the information manager, and

(vii) set out that on termination of the agreement

(A) the personal health information to which the agreement applies must be transferred to the custodian, in an electronic format that the custodian can readily use, while

(I) ensuring ongoing access to the personal health information by the custodian, and

(II) requiring the information manager to cooperate fully with the custodian during the transfer, and

(B) following completion of the transfer, the information manager must securely destroy all records of the personal health information to which the agreement applies that remain in its custody.