Yukon Information and Privacy Commissioner

Health Information Privacy and Management Act

Regulations - Public Consultation

Information and Privacy Commissioner's Comments

Opening Remarks

The *Health Information Privacy and Management Act* (HIPMA) was passed by the Yukon Legislative Assembly in December of 2013. Section 127 of the HIPMA authorizes the Commissioner in Executive Council to make regulations that are "necessary or advisable to carry out the purposes of the HIPMA." The regulations the Commissioner can make include 68 that are expressly set out in section 127 of the HIPMA.

In September 2015, the Yukon Government, Department of Health and Social Services (HSS) issued a public discussion document (Discussion Document) requesting public feedback on the development of regulations under the HIPMA. Four topic areas were identified in the Discussion Document as the areas HSS is seeking public feedback on for development of the HIPMA regulations. These four topic areas are as follows.

Topic #1 Who should be prescribed in the regulations as a custodian.

Topic #2 Who should be prescribed in the regulations the ability to require production of an individual's Yukon Health Care Insurance Plan Card.

Topic #3 The information security standards that should be prescribed in the regulations for effective security of personal health information in the custody or control of a custodian and what should be contained in an agreement entered into between custodians and researchers or information managers to ensure protection of the personal health information subject to the agreement.

Topic #4 The maximum fees that should be prescribed for an individual to access his or her own personal health information.

As previously noted, there are 68 regulations set out in section 127 of the HIPMA. The topics identified in the Discussion Document address only a few. My comments, which follow, touch on those regulations proposed for development under the HIPMA and the implications to Yukoners for not developing certain regulations contained in section 127.

My comments are divided into two sections. The first section contains my comments about what is being proposed in discussion topic #2 and on the decision not to develop a regulation as permitted by section 79 of the HIPMA that enables Yukoners to use consent directives as a measure for increased privacy protection for personal health information accessible through the Yukon health information network. The second section contains my comments by subsection in respect of the regulations authorized for development under section 127.

The references to sections, subsections, and paragraphs below are to the HIPMA unless otherwise stated.

Section One Comments

Yukon Health Insurance Plan Number and Card

In discussion topic #2 – How Private Should Your Health Card Be, the following is proposed.

> *Consider allowing other uses of your Yukon health card for various government and non-government programs and services.*

Examples provided for such use are by the Department of Environment to obtain a hunting licence and by the Yukon Film & Sound Commission for the purposes of the Film Publication Fund.

Subsection 18 (1) prohibits any person from collecting, using or disclosing a Yukon Health Care Insurance Plan (YHCIP) number except for the purposes identified in subsection 18 (2) which are primarily health related.

> ***18** (2) Subsection (1) does not apply to the collection, use or disclosure of an individual's Yukon public health insurance plan number*
>
> *(a) in relation to the provision of publicly funded health care to the individual;*
>
> *(b) for health research or a designated investigation;*
>
> *(c) for a purpose related to the Yukon health information network;*
>
> *(d) for a purpose related to a prescribed enactment;*
>
> *(e) for the purpose of a proceeding;*
>
> *(f) by the Canadian Institute for Health Information or by a prescribed health data institute in Canada that has entered into an agreement described in paragraph 58(o) that applies in respect of the number; or*
>
> *(g) for a prescribed purpose.*

Subsection 18 (3) prohibits the ability of any person to request production of a YHCIP card except for health related purposes identified in paragraph 18 (4)(a) and as prescribed under paragraph 18 (4)(b).

> ***18** (4) A custodian, agent of a custodian or prescribed person may request production of a YHCIP card*
>
> *(a) in relation to the provision of publicly funded health care to the individual; or*
>
> *(b) for a prescribed purpose.*

Subsection 7 (1) states the following:

> ***7** (1) Except as provided in subsection (2), this Act applies to*
>
> *(b) the collection, use or disclosure by any person of a Yukon public health insurance plan number; and*
>
> *(c) a request made by any person for the production of a YHCIP card.* [My emphasis]

The definition of "person" in section 2 includes government and non-government bodies.

What is being proposed in the Discussion Document presents significant risks to Yukoners given the highly sensitive nature of a YHCIP number and card. As was pointed out in the explanation accompanying the discussion topic, "**Your health card number is the gateway to your personal health information**." This reality should not be taken lightly and I strongly encourage Yukoners not to support the proposal. My reasons for this, which are numbered one through five, are set out below.

1. **All other jurisdictions in Canada with health information privacy legislation restrict or prohibit the collection, use and disclosure of health care insurance numbers and cards except for health related purposes.**

2. **Canadian health care insurance numbers and cards are a wanted commodity by identity thieves and the harm that can result from a breach of personal health information can be significant.**

A study conducted by Ponemon Institute[1] in 2014 found that "cybercriminal attacks on healthcare organizations have doubled in the past three years." They also noted that "according to experts, medical identities are precious commodities on the black market, more valuable than financial identities."[2]

The Government of British Columbia recently discovered it had more than nine million health care cards in circulation for only five million residents. It was estimated that approximately $260 million per year was being lost to fraud.[3] The Canadian Health Care Anti-fraud Association estimated that as of January 3, 2013, between two and ten percent of every health care dollar in North America is lost to fraud.[4]

A recent article identified the following about the risks associated with medical identity theft and fraud.

> *Medical identity theft is when someone uses your personal information to seek medical services.*
>
> *Unlike the traditional form of identity theft, where your financial health and good name is in jeopardy, medical identity theft can have a much more detrimental outcome. Medical identity theft can threaten your health and your life. If the thief's health information is mixed with yours, your treatment, your insurance and your payment records, may be affected.*

---

[1] "Ponemon Institute conducts independent research on privacy, data protection and information security policy. Ponemon Institute is the parent organization of the Responsible Information Management (RIM) Council." "The RIM Council draws its name from the practice of Responsible Information Management, an ethics-based framework and long-term strategy for managing personal and sensitive employee, customer and business information." This and more information about Ponemon Institute can be found on their website located at: http://www.ponemon.org/.

[2] Risks and Cyber Threats to Healthcare Industry, September 16, 2014, INFOSEC Institute website, located at: http://resources.infosecinstitute.com/risks-cyber-threats-healthcare-industry/.

[3] Checking the Numbers Behind BC CareCard Fraud, Parsons, C., January 8, 2013, Technology, Thoughts & Trinkets website located at: https://www.christopher-parsons.com/checking-the-numbers-behind-bc-care-card-fraud/. This article suggests that the numbers reported by the Government of British Columbia may be inaccurate.

[4] *Ibid.*

According to police an Ontario Health care card sells for about $1,000 on the street. In 2005 Ontario government officials estimated that, there were approximately 300,000 extra unaccounted health cards issued. And of the 300,000 cards in 2005, 268,000 of those are in the Toronto area. 10,000 extra cards are in regions near the US border.

3.7% of Canadians have been data breach victims of personal health information. According to a survey of 1,002 patients in October 2011 by Fair Warning Inc. of those, 57% of victims were negatively impacted. 11% were victims of Medical Identity Theft and 11% had inaccurate medical records.

According to the World Privacy Forum, "Medical identity theft is a crime that can cause great harm to its victims. Yet despite the profound risk it carries, it is the least studied and most poorly documented of the cluster of identity theft crimes. It is also the most difficult to fix after the fact, because victims have limited rights and recourses. Medical identity theft typically leaves a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[5]

Ann Cavoukian, former Information and Privacy Commissioner of Ontario stated the following about the need to protect health information.

…nothing deserves greater protection than a patient's medical information.

In one year, the Office of the Information and Privacy Commissioner of Ontario received 135 breaches of health information privacy.

More than 3% of Canadian patients have already experienced breaches of medical information.[6]

3. The rules to protect personal health information under the HIPMA are far more robust and offer better protection of personal health information than under the *Access to Information and Protection of Privacy Act*, which applies to the Yukon government departments and other Yukon public bodies.

A comparison between the HIPMA and the *Access to Information and Protection of Privacy Act* (ATIPP Act) demonstrates that personal health information is better protected under the HIPMA.

Under the HIPMA, to ensure adequate protection of personal health information custodians are required to have in place a privacy management program consisting of the following.

---

[5] Medical Identity Theft: The Information Crime That Kills, Ryzynski, A., April 24, 2013, id Alerts Canada Inc. website, located at: http://www.idalerts.ca/blog/2013/4/24/medical-identity-theft-the-information-crime-that-kills.html

[6] A sickening side-effect of the eHealth revolution, Priest, L., January 26, 2012, The Globe and Mail website located at: http://www.theglobeandmail.com/news/politics/a-sickening-side-effect-of-the-ehealth-revolution/article1359796/.

- A custodian is required to designate a contact individual whose responsibilities include ensuring all employees of the custodian are appropriately informed of their duties under the HIPMA and responding to security breaches;[7]

- A custodian is required to have administrative policies and technical and physical safeguards including:

    - measures that protect the confidentiality, privacy, integrity and security of personal health information and prevent unauthorized modification;

    - controls that limit the individual who may use personal health information to those specifically authorized by the custodian to do so;

    - controls to ensure that personal health information cannot be used unless 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 the proposed use is authorized,

    - taking all reasonable steps to prevent a security breach;

    - providing for secure storage, disposal and destruction of records to minimize the risk of unauthorized access to, or disclosure of, personal health information; and

    - developing policies which provide that personal health information is retained in accordance with the prescribed requirements;[8]

- A custodian is required to make public a written statement of the custodian's information practices available to the public;[9]

- A custodian is required to notify individuals about a breach of their personal health information if there is a risk of significant harm to the individual and to report these breaches to the Information and Privacy Commissioner.[10]

The ATIPP, which applies to Yukon government departments and other Yukon public bodies, contains only the following requirement to protect personal health information.

> *The public body must protect personal information by making reasonable security arrangements against such risks as accidental loss or alteration, and unauthorized access, collection, use, disclosure or disposal.*[11]

In my 2014 annual report I highlighted that Yukon public bodies do not have privacy management programs in place and that "Yukon public bodies have a significant amount of work to do to ensure Yukoners' personal information is adequately protected."

[7] Section 20,
[8] Section 19.
[9] Section 21.
[10] Section 29.
[11] Section 33 of the ATIPP Act.

4. Non-governmental organizations may not be subject to any privacy laws.

As previously stated public sector entities in Yukon, such as Yukon government departments, are subject to the ATIPP Act and are required by Part 3 of that Act to protect privacy. The HIPMA, once it is proclaimed will apply to custodians in both the public sector, such as HSS and the Yukon Hospital Corporation, and in the private sector, such as health care providers including doctors and dentists. The *Personal Information Protection and Electronic Documents Act* applies to private sector organizations that are engaged in commercial activity. Most non-governmental organizations are not typically engaged in commercial activity because they operate not-for-profit. These organizations would, therefore, not be subject to any privacy laws.

5. The risks associated with a breach of a YHCIP number or card suggest it is inappropriate to collect this kind of highly sensitive personal health information for the secondary purpose of determining residency.

The explanation provided for discussion topic #2 indicates that a YHCIP card "is sometimes used to prove Yukon residency."

The personal health information appearing on a YHCIP card should only be used for health related purposes where the collection, use or disclosure of this personal information is necessary. The risks associated with a breach of this personal health information supports that it should not be used for the secondary purpose of proving residency. Further, collection of a YHCIP card for this purpose by a Yukon public body may, in any event, be unlawful.

The YHCIP card has a considerable amount of personal information on it. Each card has a YHCIP number, date of birth, sex, full name, home address, and effective date. Under section 29 of the ATIPP Act, Yukon public bodies are only authorized to collect personal information: (a) if authorized by a Yukon or Federal law, (b) for law enforcement purposes, or (c) if the information relates to and is necessary to carrying a program or activity of the public body. Most public bodies rely on subsection 29 (c) of the ATIPP Act to collect personal information.

Using one of the examples provided in the proposal, if the Department of Environment were to collect your YHCIP card, it would have to establish under subsection 29 (c) of the ATIPP Act that it has authority to collect all the personal information appearing on the card. In determining whether personal information is "necessary" to collect, the sensitivity of the information is taken into account along with the reliability. There is evidence to support that the effective date appearing on a YHCIP card, which is essentially the eligibility date for a Yukon resident to obtain YHCIP coverage, does not in every case enable a Yukon public body to determine the date of residency of the card holder.

Even if a Yukon public body were not going to "collect" the information appearing on the card by viewing the card only, there are more reliable means of determining the date of residency using far less sensitive personal information than that appearing on a YHCIP card, such as through a letter of employment or utility bill, or using this kind of less sensitive information to issue a date-of-residency card.

To answer the question posed in the discussion topic - How Private Should Your Health Card Be? My view is that, for the foregoing reasons, this card should be very private and any collection, use and disclosure or authority for production of the card should be restricted only to health care related purposes.

Consent Directives

The Discussion Document is silent on whether a regulation will be developed to facilitate the ability of Yukoners to control access to their personal health information through the Yukon health information network (YHIN).

Section 79 states the following.

> ***79*** *The Commissioner in Executive Council may by regulation establish a means by which individuals may, to the extent provided in the regulation, control access through the Yukon health information network to any of their personal health information that is YHIN information.*

Subsection 127 (2) authorizes the Commissioner in Executive Council to make regulations for a number of things including:

> *(c) as part of or in addition to any regulation under section 79 that allows individuals to control access through the Yukon health information network to their personal health information*
>
> *(i) set out procedures for the exercise of such control, or*
>
> *(ii) impose requirements on custodians and authorized users.*

In my comments on *Bill No. 61, Health Information Privacy and Management Act* (Bill 61) I stated the following about consent directives.

> *The Act does not contain any rights for an individual to create a consent directive to control access to their personal information. This ability is subject to the regulations.*
>
> *Given that Yukoners have no say in what personal health information is accessible to authorized users through the YHIN, Yukoners may wish to consider whether this right should be expressly stated in the HIPMA.*

Not all authorized users of the YHIN require access to all personal health information accessible through the YHIN for the purposes of providing health care or related to health care. Given that the HIPMA is consent based legislation, Yukoners should have the ability to create consent directives to limit access to sensitive personal health information subject to certain specified exceptions. An example follows demonstrating how consent directives may operate.

A Bill that is currently before Ontario's Legislative Assembly to amend Ontario's *Personal Health Information Protection Act* includes a significant amount of detail about how consent directives will operate in Ontario once the Bill is enacted.[12]

[12] *Bill 119, Health Information Protection Act, 2015*, is at first reading.

- Individuals will be able to make consent directives to withhold or withdraw in whole or in part their consent to collect, use and disclose their own personal health information in the electronic health record for purposes of providing or assisting in care. Individuals may modify or withdraw their consent directive.

- Prescribed organizations[13] (POs) must implement consent directives and process any modifications or withdrawals. POs have a duty to assist an individual provide sufficient detail to implement, modify or withdraw the directive.

- Health care provider custodians (HPCs) are prohibited from accessing personal health information in the electronic health record that is subject to a consent directive subject to certain exceptions. HPCs are authorized to disclose personal health information subject to a consent directive to another custodian with consent.

- HPCs may override the consent directive to prevent harm to an individual or another person only where it is not reasonably possible to obtain consent. If consent is overridden to prevent harm to others, the Ontario Information and Privacy Commissioner must be notified.

- Use and disclosure of the information accessed by consent directive override is limited to the purposes of collection.

- POs are required to notify an HPC who seeks to collect information subject to a consent directive that the information is subject to the directive. The notice must be written and the HPC, upon receipt of the notice, must notify the individual if the information is accessed in accordance with the regulations.

- POs are required to audit and monitor every instance where personal health information is collected by consent directive override.

- Personal health information subject to a consent directive may be used to notify HPCs about harmful medication interactions provided personal health information subject to the directive is not revealed.

If the provisions of the HIPMA that authorize the creation of the YHIN were brought into force without establishing the regulation under section 79 that enables Yukoners to create consent directives to control access to their personal information through the YHIN, I would be very concerned. Consequently, I recommend that these provisions not be brought into force until the regulation under section 79 is developed and proper consultation on the development occurs.

[13] An organization prescribed under Bill 119 to create and maintain Ontario's electronic health record.

Section Two Comments

Section 127 Regulations	Provision regulation stems from	Regulations proposed Y/N	Comments
(a) a person to be, or not to be, an agent of a custodian;	**2**(1) In this Act "agent" of a custodian means a person (other than a person who is prescribed not to be an agent of the custodian) who acts for or on behalf of the custodian in respect of personal health information, including for greater certainty such a person who is (g) a **prescribed person**;	N	No comments
(b) registration information to be contact information;	**2**(1) In this Act "contact information" means **prescribed registration information;**	N	No comments
(c) a person to be, or not to be, a custodian;	**2**(1) In this Act "custodian" means a person (other than a person who is prescribed not to be a custodian) who is (g) a **prescribed person**;	Y	In topic #1 it is proposed that the following be prescribed in the regulations for paragraph 2 (1)"custodian"(g) as custodians: • Yukon Emergency Medical Services (YEMS); • Whitehorse Correctional Centre Health Centre (WCCHC); • Child Development Centre; • Many Rivers Counseling Services; • Occupational therapists; • Psychologists; • Naturopaths; and • Others? It is unclear from the proposal if the YEMS, and WCCHC, which are within public bodies as defined in the ATIPP Act, and the Child Development Centre and Many Rivers Counseling Service, which are non-profit organizations, will be prescribed in the regulations as "health facilities." If not, consideration should be given to doing so if these

			custodians will have other custodians, such as health care providers, working or performing services for them. Defining them as "health facilities" will ensure it is clear who is accountable under the HIPMA for the privacy and management of the personal health information. See comments below in s.127 (j).
(d) a branch, operation or program of a Yukon First Nation to be a custodian;	**2**(1) In this Act "custodian" means a person (other than a person who is prescribed not to be a custodian) who is (d) a **prescribed branch, operation or program of a Yukon First Nation**,	Proposed (Nov 2015)	In topic #1 it is proposed that First Nations health departments be prescribed in the regulations for paragraph 2(1)"custodian"(d) as custodians. The same comments above under 127 (c) above apply if First Nations health departments will have custodians employed or preforming services for them.
(e) a person whose systematic investigation of personal health information is a designated investigation;	**2**(1) In this Act "designated investigation" means a systematic investigation of personal health information that is (a) undertaken by the Department, the Yukon Hospital Corporation or **a prescribed person,** for planning and management of the health system,	N	No comments
(f) a purpose for which, or circumstances in which, a systematic investigation of personal health information is a designated investigation;	**2**(1) In this Act "designated investigation" means a systematic investigation of personal health information that is (b) undertaken for **prescribed purposes** or in **prescribed circumstances;**	N	No comments
(g) an activity not to be health care;	**2**(1) In this Act "health care" means any activity (**other than an activity that is prescribed not to be health care**) that is or includes	N	No comments
(h) a purpose for which the provision of an observation, examination,	**2**(1) In this Act "health care" means any activity (other than an activity that is prescribed not to be health	N	No comments

assessment, care, procedure or other service is health care;	care) that is or includes (a) any service (including any observation, examination, assessment, care, or procedure) that is provided (iv) for any **prescribed purpose**		
(i) a person to be a health care provider;	**2**(1) In this Act "health care provider" means (l) a **prescribed person**;	Proposed (Nov 2015)	In topic #1 it is proposed that the following be prescribed in the regulations for paragraph 2 (1)"health care provider"(l) as health care providers: • occupational therapists, • psychologists, • naturopaths, • other? I have no comments on what is proposed.
(j) a facility to be a health facility;	**2**(1) In this Act "health facility" means (d) a **prescribed facility**;	N	See my comments under subsections 127 (c) and (d) above.
(k) identifying information to be health information;	**2**(1) In this Act "health information" of an individual means identifying information of the individual, in unrecorded or recorded form, that (e) is **prescribed**;	N	No comments
(l) a person not to be an information manager;	**2**(1) In this Act "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…	N	No comments
(m) a service the provision of which by a person causes the person to be an information manager;	**2**(1) In this Act "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 (d) **provides a prescribed service**;	N	No comments

(n) a branch, operation or program of a public body, or of a Yukon First Nation, to be a person;	**2**(1) In this Act "person" includes (b) any public body, **or any prescribed branch, operation or program of a public body**, and (c) any **prescribed branch, operation or program of a Yukon First Nation**;	Proposed (Nov 2015)	Further to my comments under subsections 127 (c) and (d) above, consideration should be given to prescribing in the regulations for paragraphs 2 (1)"person"(b) and (c), respectively, YEMS, WCCHC and First Nation health departments as persons.
(o) registration information or provider registry information to be, or not to be, personal health information;	**2**(1) In this Act "personal health information" of an individual means (b) **except as prescribed, prescribed registration information and prescribed provider registry information** in respect of the individual;	N	No comments
(p) information that must be included in a record of user activity;	**2**(1) In this Act "record of user activity" means a record created in accordance with subsection 22(3); **22**(3) A custodian must create and maintain, or cause to be created and maintained, for any electronic information system the custodian uses to maintain personal health information, a record of user activity that includes, in respect of each incident of access by a person, through the system, to personal health information or personal information (a) the person's user identification; (b) the date and time of the incident; (c) a description of the information that is accessed or that could have been accessed; and (d) any **prescribed information**	Proposed (Nov 2015)	I have no comments on what is proposed in topic #3 as it relates to paragraph 22 (3)(d). My comments, which follow, are my views on what should be prescribed in the regulations for paragraph 22 (3)(d). Consideration should be given to prescribing in the regulations for paragraph 22 (3)(d) a requirement that the amount of time a user accessed the system is maintained. This information has proven important when investigating allegations of unauthorized access.
(q) for the purposes of subsection 4(1) (i) a health facility	**4**(1) For the purposes of this Act (a) a health care provider who admits a patient to, provides health care to a patient at, or discharges a patient from a health	N	See my comments under 127 (c) and (d) above.

to which the subsection applies, or (ii) circumstances in which, or a person to whom, the subsection does not apply;	facility **prescribed for the purposes of this subsection** or a hospital is deemed to be, in doing so, an agent of the health facility or hospital; and (b) a person who is an information manager for or on behalf of a custodian is deemed to be an agent of the custodian. (2) Subsection (1) does not apply to a **prescribed person** or in **prescribed circumstances.**		
(r) personal health information, or a record containing personal health information, to which this Act does not apply;	**7**(1) Except as provided in subsection (2), this Act applies to… (2) This Act does not apply (c) to personal health information, or to a **record that contains personal health information, that is prescribed** or that is collected, used or disclosed in prescribed circumstances;	N	No comments
(s) circumstances in which this Act does not apply to the collection, use or disclosure of personal health information;	**7**(1) Except as provided in subsection (2), this Act applies to… (2) This Act does not apply (c) to personal health information, or to a record that contains personal health information, that is prescribed or that is **collected, used or disclosed in prescribed circumstances;**	N	No comments
(t) a purpose for which the Minister or the Department may collect, use or disclose personal health information without being subject to this Act;	**7**(1) Except as provided in subsection (2), this Act applies to… (2) This Act does not apply (d) to the collection, use or disclosure of personal health information by the **Minister, or the Department, for a prescribed purpose;**	N	No comments
(u) a purpose for which, or an enactment for the	**18**(1) Subject to subsection (2), no person may collect, use or disclose an individual's	Proposed (Nov 2015)	See my comments about this proposal in the section one comments above.

purposes of which, a person may collect, use or disclose an individual's Yukon public health insurance plan number;	Yukon public health insurance plan number. (2) Subsection (1) does not apply to the collection, use or disclosure of an individual's Yukon public health insurance plan number (a) in relation to the provision of publicly funded health care to the individual; (b) for health research or a designated investigation; (c) for a purpose related to the Yukon health information network; (d) **for a purpose related to a prescribed enactment**; (e) for the purpose of a proceeding; (f) by the Canadian Institute for Health Information or by a prescribed health data institute in Canada that has entered into an agreement described in paragraph 58(o) that applies in respect of the number; or (g) **for a prescribed purpose.** (3) Subject to subsection (4), no person may request production of a YHCIP card. (see below)		
(v) a person who may request the production of a YHCIP card, or a purpose for which such a person or a custodian or agent of a custodian may request its production;	**18**(1) Subject to subsection (2), no person may collect, use or disclose an individual's Yukon public health insurance plan number. (2) Subsection (1) does not apply to the collection, use or disclosure of an individual's Yukon public health insurance plan number (a) in relation to the provision of publicly funded health care to the individual; (b) for health research or a designated investigation; (c) for a purpose related to the Yukon health information network;	Proposed (Nov 2015)	See my comments about this proposal in the section one comments above.

	(d) for a purpose related to a prescribed enactment; (e) for the purpose of a proceeding; (f) by the Canadian Institute for Health Information or by a prescribed health data institute in Canada that has entered into an agreement described in paragraph 58(o) that applies in respect of the number; or (g) for a prescribed purpose. (3) Subject to subsection (4), no person may request production of a YHCIP card. (4) A custodian, agent of a custodian or **prescribed person** may request production of a YHCIP card (a) in relation to the provision of publicly funded health care to the individual; or (b) **for a prescribed purpose.**		
(w) standards in respect of information practices;	**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.** (See 19 (3) below for measures and controls required)	Proposed (Nov 2015)	Under the explanation for topic #3 – What Standards are Necessary for Managing Personal Health Information it states "the standards established by these national organizations will be used as the basis for establishing more general regulations for Yukon custodians." The examples provided are the Canadian Medical Association and the Canadian Nurses Association. There is a recognized international standard for the security of health information developed by the International Standards Organization (ISO). This standard has been adopted by numerous health care organizations across Canada. Information about this standard follows. *ISO 27799:2008 specifies a set of detailed controls for managing health information security and provides health information security best practice guidelines. By implementing this International Standard, healthcare organizations and other custodians of health information will be able to ensure a minimum requisite level of security that is appropriate to their organization's*

			circumstances and that will maintain the confidentiality, integrity and availability of personal health information. *ISO 27799:2008 applies to health information in all its aspects; whatever form the information takes (words and numbers, sound recordings, drawings, video and medical images), whatever means are used to store it (printing or writing on paper or electronic storage) and whatever means are used to transmit it (by hand, via fax, over computer networks or by post), as the information must always be appropriately protected.*[14] Consideration should be given to prescribing in the regulations ISO 27799, as amended from time to time, as the standard for subsection 19 (2) on which custodians will be required to base their information practices. The standards in ISO 27799 should be evaluated to formulate the requirements to include in the regulation.
(x) requirements that custodians must meet under section 19 in respect of personal health information that is in their custody or control;	**19** (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	Proposed (Nov 2015)	In topic #3 - What Standards are Necessary for Managing Personal Health Information it states that the regulations may require custodians to develop and operate within written privacy and security policies and procedures which contain the following: • how to protect personal health information during its collection, use and disclosure, • how personal information on removable media will be used to record this information and how it will be securely stored, • how personal health information is secured when stored to prevent unauthorized access, • how a custodian will track access to personal health information in order identify breaches of security, • how and when training will occur. My comments on Bill 61 indicated there is a need to require custodians undertake proactive compliance measures to mitigate the risks to privacy. On this

[14] *ISO 27799:2005 Health Informatics – Information security management in health using ISO/IEC 27002*, International Standards Organization website: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=41298.

	(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.		point I stated the following about the need for custodians to use a privacy impact assessment (PIA) as a proactive measure for privacy risk mitigation. *…a PIA is a risk management tool that assists in identifying and managing risks of non-compliance with privacy legislation. PIAs are used to evaluate the risks associated with any new practice, changes to an existing practice or to an information system involving the collection, use or disclosure of personal health information. A PIA requires the author to identify and reduce or eliminate the privacy risks identified. One of the requirements of a PIA is that the custodian must identify the privacy policies, procedures and training In place to facilitate compliance with privacy legislation.* *PIAs have proven to be one of the best measures to promote proactive compliance with health privacy legislation.* I then recommended that HIPMA incorporate the following two requirements: 1. a requirement that custodians prepare and submit to the IPC for approval a PIA for any new administrative practices or information systems which involve the collection, use and disclosure of personal health information; and 2. a requirement that prior to making personal health information accessible through the YHIN that custodians prepare and submit a PIA to the IPC for approval. In response to this recommendation, HSS committed to including in regulation a requirement that HSS undertake PIAs on "significant new information initiatives, or changes to existing information systems." The Discussion Document is silent on whether this requirement will be included in the regulations. As such, clarification is required about whether this commitment will be met. For the reasons provided above, I will reiterate that consideration should be given to prescribing in the regulations for paragraph 19 (3)(h) a requirement that all custodians complete a PIA for any new administrative practice or information system involving the collection, use and disclosure of

			personal health information and prior to making personal health information accessible through the YHIN, and that these PIAs be submitted to the IPC for review and comment.

(y) functions or duties of contact individuals;	**20**(1) Except as provided in subsection (3), a custodian must designate at least one individual (referred to in this section as the custodian's "contact individual") for the purposes of this section.
	
	(2) A custodian's contact individual must
	
	(a) receive and process complaints from the public about the custodian's information practices;
	
	(b) respond to requests for access to, or correction of, a record of an individual's personal health information that is in the custody or control of the custodian;
	
	(c) ensure that all agents of the custodian are appropriately informed of their duties under this Act;
	
	(d) respond, in respect of security breaches, to individuals whom the custodian has notified under section 30 and to the commissioner; and
	
	(e) **perform any prescribed functions or duties.**
	
	(3) A custodian who is an individual and who does not designate a contact individual under subsection (1) is deemed to be their own contact individual, and must perform the functions described in subsection (2).
		N	In addition to the functions and duties of a contact individual as stated in section 20, to ensure effective management of personal health information, the functions and duties of a custodian's contact individual that should be prescribed in the regulations for paragraph 20 (1)(e) are as follows.
			
			The contact individual should be required to establish a personal health information management program (Program) comprised of:
			
			• a personal health information inventory;
			• privacy policies and procedures that identify:
			  • the purpose and authority for collection, use and disclosure of personal health information;
			  • how to ensure accuracy of personal health information;
			  • how to facilitate access to and correction of personal health information;
			  • retention and destruction or disposal of personal health information;
			  • how personal health information will be secured;
			  • how a privacy breach will be managed, and
			  • how complaints will be managed;
			  • use of risk assessment tools, such as PIAs and security threat risk assessments;
			  • training of new staff and existing staff when changes to policy and procedure occur;
			  • management of contracts to ensure risks to privacy are adequately addressed through the contract; and
			  • how patients or others will be informed about how the custodian is protecting privacy;
			• a plan to revie*w* the effectiveness of the Program including the policies and procedures;

			• reporting on the effectiveness of the plan; and • a plan to update the Program as necessary.[15]
(z) requirements for custodians' written statements under section 21 or records of user activity under section 22;	**21** A custodian must make available to the public a written statement that (a) provides a general description of the custodian's information practices; (b) describes how to contact the custodian's contact individual; (c) describes how an individual may obtain access to, or request an annotation for the correction of, a record of their personal health information that is in the custody or control of the custodian; (d) describes how to make a complaint to the custodian and how to make a complaint to the commissioner under this Act; and (e) **meets the prescribed requirements**, if any. **22**(1) If a custodian discloses any of an individual's personal health information to a person without the individual's consent, the custodian must record (a) the name of the person; (b) the date and purpose of the disclosure; and (c) a brief description of the personal health information. (2) Subsection (1) does not apply to the disclosure of a record that contains only registration information or provider registry information. (3) A custodian must create and maintain, or cause to be created and maintained, for any	Proposed (Nov 2015)	I have no comments for section 21 and subsection 22 (4). For paragraph 22 (3)(d), see my comments under s. 127 (p) above.

[15] Guidance for Public Bodies on Accountable Privacy Management, Yukon Information and Privacy Commissioner, January 29, 2015, Information and Privacy Commissioner's website: http://www.ombudsman.yk.ca/uploads/media/55f99c6eed395/Guidance%20Privacy%20Management%20Program.pdf?v1.

	electronic information system the custodian uses to maintain personal health information, a record of user activity that includes, in respect of each incident of access by a person, through the system, to personal health information or personal information (a) the person's user identification; (b) the date and time of the incident; (c) a description of the information that is accessed or that could have been accessed; and (d) **any prescribed information**. (4) A record of user activity under subsection (3) must meet the **prescribed requirements**, if any.		
(aa) a person to whom custodians may transfer custody and control of personal health information or records containing personal health information, and requirements in respect of such transfers;	**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. (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 the custodian in accordance with section 60 or to a **prescribed person in accordance with the prescribed requirements, if any**.	N	For subsection 23 (1), consideration should be given to prescribing in the regulations the requirements that must be met to properly secure personal health information during the transfer of custody or control of personal health information to a successor custodian. I have no comments for subsection 23 (2).
(bb) the maximum amount (or a formula for determining the	**24**(1) Subject to this Part, an individual has the right to obtain access to their personal health information contained in a record in the custody or control of a custodian.	Proposed (Nov 2014)	The proposal in topic #4 is to establish the maximum fees a custodian can charge an individual for access to his or her own personal health information.

maximum amount) that a custodian may charge an individual for access to the individual's personal health information;	(2) A custodian may charge a fee, not exceeding the **prescribed fee**, for access to personal health information contained in a record in the custody or control of the custodian.		I have no comments on what is proposed.
(cc) limitations on the availability to an individual of a record of user activity of the individual's personal health information;	**24** (3) If a custodian uses electronic means to collect, use or disclose an individual's personal health information (a) the right of access includes, subject to any **prescribed limitations**, the right to obtain a copy of a record of user activity of the individual's personal health information;	N	No comments
(dd) requirements for applications under section 25;	**25**(1) An individual who seeks access to their personal health information contained in a record in the custody or control of a custodian may apply to the custodian in accordance with this section. (2) An application under this section is complete only if (a) it is made in writing, unless the custodian agrees otherwise; (b) it contains sufficient detail to enable the custodian to identify the personal health information requested; (c) in a case where the applicant seeks a record of user activity of the applicant's personal health information, the application indicates that a record of user activity is sought; and (d) it meets the **prescribed requirements, if any.**	Proposed (Nov 2014)	Subsection "25 [(2)](d)" is referenced in topic #4. I have no comments regarding what is proposed as it relates to this subsection.
(ee) additional factors that are to be considered in determining whether a	**30** (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	N	Due to Yukon's small population, an important factor in Yukon when determining whether harm may occur as a result of a breach is whether there is a personal relationship between the person who had unauthorized access to personal health

custodian has reasonable grounds to believe that an individual is at risk of significant harm as a result of a security breach;	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**.		information and the individual the information is about. Where a personal relationship exists, the individual affected by the breach can suffer reputational damage, embarrassment, and humiliation. Consideration should be given to prescribing this as a factor in the regulations for paragraph 30 (3)(g).
(ff) requirements in respect of express consent, including but not limited to circumstances in which, or purposes for which, express consent is required for the collection, use or disclosure of personal health information;	**34** Express consent is required for the collection, use or disclosure of personal health information (a) for fund-raising activities; and (b) in **prescribed circumstances** or where the collection, use or disclosure is for **prescribed purposes**.	N	No comments

(gg) requirements for a custodian's notice under subsection 41(1);	**41**(1) Except as provided in subsection (2), a custodian is entitled to assume that an individual's consent to the collection, use or disclosure of the individual's personal health information is knowledgeable if the custodian has posted, in a place where it is likely to come to the individual's attention, or makes readily available to the individual, a notice that meets the **prescribed requirements**, if any, and that (a) describes the purpose of the collection, use or disclosure; (b) advises that the individual may, with respect to the collection, use or disclosure of their personal health information for the purpose of providing health care to them, give or withhold consent and having once given consent, may withdraw that consent (c) confirms that without the individual's consent the personal health information can be collected, used or disclosed only in accordance with the provisions of this Act and the regulations; and (d) advises that if the personal health information is disclosed outside Yukon, the law of the jurisdiction to which it is disclosed will govern its use, collection and disclosure in that jurisdiction.	N	No comments
(hh) requirements for an individual's withdrawal of consent under section 42;	**42** (1) An individual may withdraw their consent to a custodian's collection, use or disclosure of the individual's personal health information by notifying the custodian who has the custody or control of the personal health information. (2) An individual's withdrawal of consent under subsection (1) (a) must meet the **prescribed requirements**, if any; and (b) does not apply to the collection, use or disclosure of the individual's personal health information by any custodian before that	N	No comments

	custodian received notice of the withdrawal of consent.		
(ii) information that a custodian must provide to an individual whose refusal or withdrawal of consent the custodian refuses to comply with;	**42** (3) If a custodian refuses under subsection (2) to comply with an individual's refusal or withdrawal of consent, the custodian must (a) inform the individual as soon as reasonably possible that the custodian has refused to comply; (b) upon request of the individual make reasonable efforts to inform the individual of the identity of each other person to whom the custodian has, during the year before the custodian received the individual's request, disclosed the personal health information; and (c) provide the individual with all other information, if any, that is **prescribed**.	N	Consideration should be given to prescribing in the regulations for paragraph 42 (3)(c) a requirement that Custodians inform the individual about their ability to make a complaint to the IPC about the refusal by the custodian to comply with an individual's refusal or withdrawal of consent
(jj) exceptions to, or otherwise modify, the requirements of subsection 46(2) in respect of substitute decision-makers;	**46** (1) In this section, "close friend" of an individual means a person who, through frequent personal contact and a personal interest in the individual's welfare, maintains a long-term close personal relationship with the individual. (2) Unless a **regulation** provides otherwise, if reference is made under this Act to an individual's consent to a custodian's collection, use or disclosure of the individual's personal health information, and the individual is incapable of giving the consent, the custodian must choose as the individual's substitute decision-maker for the consent the first individual in the following list who is willing and able to perform that function	N	No comments
(kk) requirements under paragraph 50(1)(d) for an agent's collection, use, disclosure, retention, destruction or	**50** (1) A custodian may permit its agent to collect, use, disclose, retain, destroy or dispose of personal health information on the custodian's behalf only if (a) the custodian is permitted or required to collect, use, disclose, retain, destroy or	N	No comments

disposal of personal health information;	dispose of the information, as the case may be; (b) the collection, use, disclosure, retention, destruction or disposition of the information, as the case may be, is in the course of the agent's duties and is not contrary to the limits imposed by the custodian, this Act or any other enactment; (c) the custodian allows the agent to use only that personal health information that the agent needs in order to carry out the purpose for which it was collected or a purpose for which use is authorized under this Act; and (d) the **prescribed requirements**, if any, are met.		
(ll) requirements in respect of a custodian's retention of the services of an information manager;	**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.	Proposed (Nov 2015)	It is proposed in topic #3, that a service agreement entered into with an information manager (IM) must: • state that the custodian controls the personal health information, • identify the services to be provided to the custodian by the IM, and • set out the responsibilities for the custodian and the IM and the obligation to comply with the HIPMA. In addition to the foregoing, consideration should be given to prescribing in the regulations for paragraph 51 (1)(b) that a service agreement entered into with an IM also must: • require the IM to limit access to the information and restrict any uses and disclosures of personal health information; • require the IM to follow the custodian's policies and procedures for privacy protection; • ensure that the IM has in place appropriate authentication and access controls and that staff of the IM with access sign confidentiality agreements in respect of any access to personal health information;

			• if personal health information will be transmitted, ensure encryption is used; • define the process to manage a privacy breach that includes timely notification about a breach to the custodian and the individuals who will be responsible for managing the breach; • ensure that any testing of the IM services that require data is done using data other than personal health information; • ensure the custodian is able to audit the IM's responsibilities for privacy protection under the agreement and the procedure used for this audit; and • restrict subcontracting by the IM for services unless the custodian consents.
(mm) requirements with which an information manager must comply under subsection 51(2);	**51** (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 requirement**s, if any; and (b) notify the custodian at the first reasonable opportunity of any breach of the agreement by the information manager.	Proposed (Nov 2015)	See my comments under subsection 127 (ll) above.
(nn) requirements or restrictions in respect of the collection from a person other than the individual, use or disclosure of personal health information under an enactment of Yukon or Canada, or a treaty, agreement or arrangement made pursuant to such an	**54** A custodian may collect an individual's personal health information from a person other than the individual only if (a) the individual consents to the collection; (b) where the custodian collects the personal health information for the purpose of providing health care to the individual, the personal health information is reasonably necessary for that purpose and the custodian reasonably believes that collection directly from the individual (i) would prejudice the purposes of collection, (ii) would delay the collection in circumstances where delay would negatively	N	No comments

enactment;	affect the custodian's ability to provide necessary health care to the individual on a timely basis, (iii) could result in the collection of information that is not accurate, or (iv) is not reasonably practicable in the circumstances; or (c) where the custodian collects the personal health information for a purpose other than providing health care to the individual (i) section 56 (other than its paragraph (1)(g), (h) or (l), (3)(a) or (7)(b)) allows the custodian to use the personal health information for that other purpose without the individual's consent, (ii) the custodian reasonably believes that collection from the individual could cause serious harm to the health or safety of any individual, iii) the custodian reasonably believes that the individual is or may become the substitute decision-maker of, or is a relative or close friend of, another individual to whom the custodian is providing or reasonably expects to provide health care, and the personal health information is limited to contact information, (iv) **subject to the requirements and restrictions, if any, that are prescribed, in an enactment of Yukon or Canada, or a treaty, agreement or arrangement** made pursuant to such an enactment, permits or requires the collection, (see below for more)		
(oo) circumstances in which, or purposes for which, a custodian may collect an	(v) the personal health information is available to the public, or (vi) the personal health information is **collected in prescribed circumstances or for prescribed purposes.**	N	No comments

individual's personal health information, from a person other than the individual, without the individual's consent and for a purpose other than providing health care to the individual;			
(pp) circumstances in which the determination, assessment or confirmation of the individual's capacity is a purpose for which a custodian may, without an individual's consent, use or disclose to another custodian the individual's personal health information;	**56** (1) A custodian may, without an individual's consent, use the individual's personal health information that is in its custody or control (k) for the purpose of determining, assessing or confirming the individual's capacity, if the determination, assessment or confirmation (ii) is conducted in **prescribed circumstances;**	N	No comments
(qq) an enactment in relation to which a custodian may use or disclose an individual's personal health information as described in paragraph (pp);	**56** (1) A custodian may, without an individual's consent, use the individual's personal health information that is in its custody or control (k) for the purpose of determining, assessing or confirming the individual's capacity, if the determination, assessment or confirmation (i) relates to the application of this Act, the *Care Consent Act*, the *Access to Information and Protection of Privacy Act*, the *Adult Protection and Decision-Making Act*, the *Mental Health Act*, the *Enduring Power of Attorney Act* or any **prescribed enactment**	N	No comments

	of Yukon or Canada,		
(rr) a purpose, other than providing health care to the individual, for which a custodian may use an individual's personal health information without the individual's consent;	**56** (1) A custodian may, without an individual's consent, use the individual's personal health information that is in its custody or control (q) for any **prescribed purpose**.	N	No comments
(ss) a branch, operation or program of a public body that may use, or to which a custodian may disclose, an individual's personal health information for the planning and management of the health system, and limits on that use;	**56** (4) The Minister, the Department, the Yukon Hospital Corporation or a **prescribed branch, operation or program of a public body may**, without an individual's consent, use the individual's personal health information for the purpose of the planning and management of the health system.	N	No comments
(tt) circumstances in which, and persons to whom, a custodian must disclose an individual's personal health information if the individual consents to the disclosure, and requirements for such consent;	**57** (2) In **prescribed circumstances** a custodian must disclose to a prescribed person an individual's personal health information if the individual consents to the disclosure.	N	No comments

(uu) a health data institute;	**58** A custodian may disclose an individual's personal health information without the individual's consent (n) to the Canadian Institute for Health Information, or to a **prescribed health data institute** in Canada that has entered into a written agreement with the Minister governing its collection, use and disclosure of the personal health information;	N	No comments
(vv) a person whose funding of goods, services or benefits is relevant for the purposes of paragraph 58(p) or (q);	**58** A custodian may disclose an individual's personal health information without the individual's consent (p) to another custodian, for the purpose of determining or verifying an individual's eligibility to receive health care or other related goods, services or benefits funded in whole or in part by the Government of Yukon, the government of another province or Canada or a **prescribed person**;	N	No comments
(ww) personal health information that a custodian may disclose (i) to the police, for the purpose of assisting in locating an individual who is, or is reasonably believed to be, missing, or (ii) to the police or the Minister of Justice, in relation to an offence or a possible offence;	**58** A custodian may disclose an individual's personal health information without the individual's consent (w) if the individual is missing or reasonably believed to be missing, to the police for the purpose of assistance in locating the individual, if the personal health information disclosed is limited to (i) registration information of the individual, (ii) the date the custodian's records show that health care was last provided to the individual, the individual's general health status at that time and the identity of the person who provided that health care, and (iii) **any prescribed information**; (x) to the Minister of Justice or the police, if the personal health information (i) relates to the possible commission of an offence under an enactment of Yukon or	N	No comments

	Canada, or is required in anticipation of the laying of an information in relation to, or is for use in the prosecution of such an offence, and (ii) is limited to the **prescribed information;**		
(xx) a person to whom a custodian may disclose personal health information for the purpose of operating the Yukon health information network;	**58** A custodian may disclose an individual's personal health information without the individual's consent (ee) if the custodian is the Minister, the Department, the Yukon Hospital Corporation or a **prescribed person**, and the disclosure is for the purpose of the Yukon health information network.	N	No comments
(yy) in respect of diagnosis decisions under section 61 (i) a health care provider whose report may be used in support of a court order under the section, or (ii) conditions for such an order;	**61** (2) The court may, upon application in accordance with this section and the Rules of Court made under the *Judicature Act*, order that a source individual or any other person disclose, for the purpose of a diagnosis decision, any of the source individual's personal health information (5) No report of a proceeding under this section in which the name or identity of the affected individual or of the source individual is indicated may be published, broadcast or in any other way made public by any person without the leave of the court. (6) An order may be made under subsection (2) only if (a) the report of a medical practitioner or other prescribed health care provider indicates that the diagnosis decision cannot be made conclusively without the personal health information sought; (e) any **prescribed conditions** that apply are met.	N	No comments

(zz) information to be follow-up care information for the purposes of section 62;	**62** (1) "follow-up care information" for an individual means (e) any **prescribed information**.	N	No comments
(aaa) a person to whom the Minister may require a custodian to disclose personal health information;	**64** (2) The Minister may, subject to section 73, require a custodian to disclose, for a specified purpose, personal health information to the Department or a **prescribed person**.	N	No comments
(bbb) a person who may establish an institutional research review committee within the meaning of section 65;	**65** In this Division, "institutional research review committee" means a committee (a) that a university, a hospital affiliated with a university or a **prescribed person** establishes	N	No comments
(ccc) a custodian as a person described in paragraph 66(2)(a), or requirements that a custodian described in that paragraph must meet in order to collect, for research purposes, an individual's personal health information from a person other than the individual;	**66** (2) If a custodian intends to collect an individual's personal health information for the purpose of research (other than research that is incidental to a purpose for which this Act otherwise allows the custodian to collect the personal health information), the custodian must (a) where the custodian is a public body, a branch, operation or program of a Yukon First Nation or a prescribed person, meet the **prescribed requirements**, if any; or	N	In my comments on Bill 61, I highlighted a need to consider requiring a custodian who is a public body, branch, operation or program of a Yukon First Nation or a prescribed person to have proposed research reviewed by an institutional research review committee (Review Committee). One of the roles of a Review Committee is to ensure the personal health information used for research has adequate safeguards in place to protect the confidentiality of personal health information.[16] This requirement was not incorporated into Bill 61. Therefore, the ability of these custodians to conduct research without any evaluation of privacy risks remains in the HIPMA. I remain concerned that without some controls on the ability of these custodians to conduct research using personal health information there are risks to privacy. To ensure privacy will be adequately protected when conducting research, consideration should be given to prescribing in the regulations for paragraph 66 (2)(a) that for research planned under paragraph

[16] See definition of "institutional review committee" in section 65 of the HIPMA.

			66 (2)(a), a custodian who is a public body, branch, operation or program of a Yukon First Nation or a prescribed person must prepare a PIA and submit it to the IPC for review and take into account any of the IPC's comments about privacy risks prior to commencing the research.
(ddd) requirements that a researcher's research must meet in order for a custodian that is a public body to disclose personal health information to the researcher;	**68** (2) A custodian that is a public body may disclose an individual's personal health information to a researcher under subsection (1) for the purposes of the researcher's research only if (a) the custodian reasonably believes that (i) the research is of sufficient importance to outweigh the intrusion into privacy that would result from the disclosure of the personal health information, (ii) the research purpose cannot reasonably be accomplished unless the personal health information is provided in a form that identifies or may identify the individual, and (iii) it is unreasonable or impractical for the researcher to obtain consent from the individual; and (b) the research meets the **prescribed requirements,** if any.	Proposed (Nov 2015)	It is proposed in topic #3 that a research agreement entered into by a custodian with a researcher must ensure the researcher. • protects the personal health information according to law (HIPMA), and • complies with additional terms and conditions respecting the collection, use and disclosure of information that a custodian may set out including things like publication limits. I do not have any comments in respect of what is proposed in relation to paragraph 68 (2)(b). My comments, which are set out in subsection 127 (eee) below, are in relation to requirements that should be prescribed for inclusion in a research agreement.
(eee) requirements for an agreement under section 69 between a custodian and a researcher;	**69** An agreement under this section between a custodian and a researcher must be in writing and must require the researcher, in respect of the personal health information to be disclosed by the custodian under subsection 68(1) (a) to maintain technical and physical safeguards to ensure the confidentiality and security of the personal health information; (b) to destroy or remove, at the earliest opportunity consistent with the purposes of the research, any identifying information; (c) not to make any subsequent use or	Proposed (Nov 2015)	As noted in subsection 127 (ddd) above, it is proposed in topic #3 that a research agreement entered into by a custodian with a researcher ensure the researcher. • protects the personal health information according to law (HIPMA), and • complies with additional terms and conditions respecting the collection, use and disclosure of information that a custodian may set out include things like publication limits. In my comments submitted in respect of Bill 61, I detailed a process associated with the ethical

	disclosure of the personal health information in individually identifiable form without the express prior authorization of the custodian; (d) not to publish any individual's personal health information in a form that could reasonably be expected to identify the individual; (e) to use the personal health information solely for the purposes of the research approved under paragraph 68(1)(a); and (f) to meet the **prescribed requirements**, if any.		review of research under the Tri-Council Policy Statement (TPS)[17] on research. In Part 5, Section C. Safeguarding Information, the TPS requires researchers to provide the ethical review body with "details…regarding their proposed measures for safeguarding information, for the full life cycle of the information: its collection, use, dissemination, retention and/or disposal."[18] The TPS provides the following factors that an ethical review body is required to consider in determining whether the proposed measures for safeguarding the information are adequate: *a. the type of information to be collected;* *b. the purpose for which the information will be used, and the purpose of any secondary use of identifiable information;* *c. limits on the use, disclosure and retention of the information;* *d. risks to participants should the security of the data be breached, including risks of re-identification of individuals;* *e. appropriate security safeguards for the full life cycle of information;* *f. any recording of observations (e.g., photographs, videos, sound recordings) in the research that may allow identification of particular participants;* *g. any anticipated uses of personal information from the research; and* *h. any anticipated linkage of data gathered in the research with other data about participants, whether those data are contained in public or personal records…*

[17] *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans, 2014, Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, Social Sciences and Humanities Research Council of Canada*, Government of Canada, Secretariat on Responsible conduct of Research, Ottawa, ON, located on the Government of Canada's website at: http://www.pre.ethics.gc.ca/pdf/eng/tcps2-2014/TCPS_2_FINAL_Web.pdf.

[18] Chapter 5 of the Tri Council Policy statement located at: http://www.pre.ethics.gc.ca/eng/policy-politique/initiatives/tcps2-eptc2/chapter5-chapitre5/.

			The TPS also indicates that researchers should put in place adequate physical, administrative and technical measures to ensure adequate protection of information. Given the foregoing, consideration should be given to including in the regulations for subsection 69 (f) the following requirements: • a requirement that the custodian include in an appendix to the agreement the measures approved by the Review Committee to safeguard the personal health information; and • a requirement that the agreement contain a provision requiring the researcher to adhere to those measures.
(fff) a purpose for which an agreement under section 70 may be entered into, or conditions that apply to the entry into such an agreement of a person described in paragraph 70(3)(d);	**70** (2) An agreement under this section must be entered into (a) for the purpose of the provision of health care, or for a **prescribed purpose**; or	N	No comments
(ggg) limitations and conditions that govern the actions of an agent as an authorized user within the meaning of section 71;	**71** (1) In this Division "authorized user" means (c) an agent of an authorized user described in paragraph (a) or (b), if the agent acts in accordance with the **prescribed limitations** and conditions, if any, and the requirements established by the Minister	N	No comments
(hhh) registration information that the Minister may require a custodian to collect, and that a	**77** (1) For the operation of the Yukon health information network or for any prescribed purpose, the Minister may require a custodian (b) to provide the **prescribed registration**	N	No comments

custodian may require an individual to provide, for the operation of the Yukon health information network;	**information** to the Minister.		
(iii) a purpose for which the requirements described in paragraph (hhh) may be imposed;	**77** (2) A custodian may require an individual who seeks health care or other related goods, services or benefits from the custodian to provide the custodian with **prescribed registration information** if the information is required to meet a requirement by the Minister under subsection (1).	N	No comments
(jjj) terms or conditions for pilot projects;	**86** (1) The Minister may operate a pilot project. (3) A pilot project is subject to any **prescribed terms or conditions.**	N	Consideration should be given to prescribing in the regulations for subsection 86 (3) a requirement that the Minister prepare a PIA for every proposed pilot project and submit the PIA to the IPC. This PIA could form the basis of the consultation with the IPC.
(kkk) information that must be included in a notice under section 90 in respect of a pilot project;	**90** At least 90 days before a pilot project begins, the Minister must (a) consult about the pilot project with, and consider the comments of, the commissioner and representatives of the custodians that may be requested to participate in the pilot project; (b) publicize the pilot project by posting, on the Internet website of the Department, a notice that describes the pilot project in generic terms and that sets out (i) the purpose of the pilot project, (ii) the proposed scope and application of the pilot project, including the custodians or classes of custodians that may be requested to participate in the pilot project, (iii) the dates proposed for the pilot project	N	Consideration should be given to prescribing in the regulations for paragraph 90 (b)(v) a requirement that the Minister include in the notice the IPC's comments and recommendations arising from the consultation.

	to start and end, (iv) the measures that will be taken during and following the pilot project for the safeguarding of personal information and personal health information, and (v) any other information that is **prescribed**; and		
(lll) duties, functions or powers of the commissioner;	**92** In addition to the specific duties and powers assigned to the commissioner under this Act, the commissioner is responsible for overseeing how this Act is administered to ensure that its purposes are achieved, and may (h) perform any **prescribed duties** or **functions or exercise any prescribed power**.	N	In my comments on Bill 61, I indicated the importance of ensuring the IPC has appropriate authority to ensure custodians are complying with the HIPMA. One of the recommendations I made in this regard is that the IPC should have authority to initiate an investigation on her own motion. In support of this recommendation I stated that: • most jurisdictions with health information privacy legislation authorize their Information and Privacy Commissioner to conduct own-motion investigations; • unless the IPC receives a complaint she has no authority to investigate even in cases where she is made aware of potential non-compliance; and • given the high sensitivity of personal health information and the harms that can flow from a breach, a complaint driven investigation model is insufficient to adequately address the risks to privacy of personal health information I also recommended that the IPC be given authority to review PIAs submitted by custodians if custodians are required to submit PIAs to the IPC for review and comment. In response to the recommendations, HSS indicated they would "include in regulation, additional powers for the Information and Privacy Commissioner." As the consultation document is silent on these powers, what is contemplated under subsection 92 (h) is unknown. Clarification is required about what will be included in the regulation about the IPC's powers.

(mmm) circumstances in which the commissioner may under subsection 101(1) refuse or cease to consider a complaint;	**101** (1) The commissioner may refuse or at any time cease to consider a complaint under this Act (b) in any **prescribed circumstances**.	N	No comments
(nnn) circumstances in which the court need not take precautions under subsection 115(4) to prevent the disclosure of personal health information or personal information;	**115** (4) In the course of an appeal, the court must take every reasonable precaution to avoid disclosure of any personal information or personal health information of an individual, except where (d) **disclosure is authorized by the regulations**.	N	No comments
(ooo) circumstances in which notice or any other document may be given to a person by substituted service.	**117** Where this Act or a regulation requires any notice or other document to be given to a person, it is to be given by (c) substituted service, if authorized by the commissioner or by a **regulation**;	N	No comments
(2) For greater certainty, in addition to the prescriptions described in subsection (1), the Commissioner in Executive Council may make regulations under this Act respecting the establishment, structure, operation, management,	**79** The Commissioner in Executive Council may by regulation establish a means by which individuals may, to the extent provided in the regulation, control access through the Yukon health information network to any of their personal health information that is YHIN information.	N	See my comments in the section one comments above on the need to establish regulations for section 79.

auditing or monitoring of the Yukon health information network and related matters, including but not limited to regulations that (a) designate a person to be a custodian in respect of personal health information; or (b) create responsibilities and duties of custodians and authorized users; (c) as part of or in addition to any regulation under section 79 that allows individuals to control access through the Yukon health information network to their personal health information (i) set out procedures for the exercise of such control, or (ii) impose requirements on custodians and authorized users.			