CONSIDERATION REPORT

File HIP16-02I

Pursuant to subsection 103 (1) of the

Health Information Privacy and Management Act

Diane McLeod-McKay, B.A., J.D.

Information and Privacy Commissioner (IPC)

Custodian: **Department of Health and Social Services**

Date: **May 18, 2018**

Summary:

The IPC received a complaint from an individual who alleged that the Department of Health and Social Services (Custodian) was collecting more personal health information from his physician for the purposes of remunerating the physician for services rendered than allowed by HIPMA. Included in the complaint was an allegation that the Custodian did not have adequate security measures in place to protect the personal health information it collected.

The IPC considered the complaint and found that the Custodian was authorized under subsection 53 (b) to collect personal health information from the physician to process the physician's billing claims and paragraphs 54 (c)(i) and 56 (1)(b) to both indirectly collect and use this personal health information for the same purpose. She also found that the Custodian met its duty under section 16 to collect the minimum amount of personal health information

it required from the physician to process the physician's billing claims submitted via its electronic billing system, but did not meet this duty for a clinic record it endeavoured to collect from the physician to process one of these claims. In terms of the security of the personal health information it collected, the IPC found the Custodian did not meet all the requirements in HIPMA.

The IPC made two recommendations. One is to evaluate the amount of personal health information it is collecting in clinic records to ensure only the minimum amount necessary to process a billing claim is collected. The second is to work in good faith with the IPC to address risks of non-compliance with HIPMA's information security requirements in the privacy impact assessment submitted to her by the Custodian.

Statutes Cited:

Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165

Health Care Insurance Plan Act, RSY 2002, c 107

Health Care Insurance Plan Regulations, YCO 1971/275

Health Information Privacy and Management Act, SY 2013, c 16

Interpretation Act, RSY 2002, c 125

Cases Cited:

British Columbia (Justice) (Re), 2014 BCIPC 29 (CanLII)

HIP16-02I Decision, Department of Health and Social Services, October 6, 2017 (YT IPC)

Rizzo & Rizzo Shoes Ltd. (Re), [1998] 1 SCR 27, 1998 CanLII 837 (SCC), at para. 21

Explanatory Notes:

All statutory provisions referenced below are to the *Health Information Privacy and Management Act* (HIPMA) unless otherwise stated.

I BACKGROUND

[1] On November 29, 2016, the Office of the Information and Privacy Commissioner (OIPC) received the following complaint from the Complainant under HIPMA:

> *Insured Health and Hearing Services (IHHS) in the Department of Health and Social Services (HSS) is collecting and using personal health information from my physician's patient files for the purpose of remunerating my physician (Physician) for services rendered contrary to HIPMA; and*
>
> *HSS does not have adequate security measures in place to protect the personal health information collected.*
>
> (Complaint)

[2] On December 8, 2016, the OIPC notified the Custodian of the Complaint.

[3] An investigator was assigned to attempt an informal settlement of the Complaint. On February 2, 2017, the investigator advised the Information and Privacy Commissioner (IPC) that settlement could not be achieved. The parties were informed and the Registrar issued a Notice of Consideration dated February 8, 2017, indicating that the consideration would occur on March 8, 2017 (Consideration).

II CONSIDERATION PROCESS

[4] Initial submissions were received from the Complainant on February 14, 2017, and from HSS on February 20, 2017. A reply submission was received from HSS on March 8, 2017. The Complainant did not submit a reply submission.

[5] After evaluating the submission received, I determined that I required more information and records from both HSS and Physician. I issued a Notice to Produce Records to each and requested an additional submission from HSS.

[6] In the Notice to Produce Records issued to Physician, I requested that he produce, *inter alia*, the following records.

> *for the period on or between August 31, 2016 and November 28, 2016* [Complaint Period] *records including correspondence, emails or other system generated forms of communication, including any containing personal health information (PHI), that were*

> *provided by Physician to Insured Health and Hearing Services in the Department of Health and Social Services (IHHS) to process Physician's billing claims;* [and]
>
> *for the period on or between August 31, 2016 and November 28, 2016* [Complaint Period] *records including correspondence* [sic] *emails or other system generated forms of communication received by Physician from IHHS during the Complaint Period requesting Physician provide IHHS with documents or other forms of information to process Physician's billing claims.*

[7] In response to this Notice to Produce Records, Physician provided me with four pages listing 200 billing claims that he submitted to IHHS during the Complaint Period.[1]

[8] On August 28, 2017, I received HSS's response to the Notice to Produce Records issued to it. Its response was that I had lost jurisdiction as a result of being out of time under section 103 to complete the Consideration. Included in its response was HSS's refusal to provide the records and submissions requested as a result of its view that I had lost jurisdiction.

[9] On October 6, 2017, I issued my decision about jurisdiction[2] in which I found that subsections 103 (2) and (3) are directory and that, as a result, I did not lose jurisdiction to complete the Consideration despite being out of time under these subsections. After issuing this decision, I instructed the Registrar to reissue the Notice to Produce Records to HSS (Notice). In the Notice I requested, *inter alia*, that it produce to me the following records.

> *correspondence or other documents including emails or other system generated forms of communication, including any containing personal health information (PHI), that were provided by* [Physician] *to Insured Health and Hearing Services (IHHS) on or between August 31, 2016 and November 28, 2016 (Complaint Period) to process his billing claims;*
>
> *correspondence or other documents including emails or other system generated forms of communication prepared or generated by IHHS during the Complaint Period requesting* [Physician] *to provide it with documents or other forms of information to process his billing claims; and*

[1] Physician produced other documents that are not relevant to this Consideration.

[2] Decision HIP16-02I, *Department of Health and Social Services*, October 6, 2017 (YT IPC).

> *policies, procedures, codes or other documents used by IHHS during the Complaint Period that support its authority to collect or use the PHI provided by or requested from* [Physician] *to process his billing claims.*

[10] On November 10, 2017, I received a letter from HSS in which it claimed it had no records to produce in response to the above requests. Specifically, it provided that an email search of employees of IHHS "did not return responsive records for this time frame." It indicated that records of suspended claims that are sent to physicians for the purpose of substantiating claims exit the system after six months and that "[i]n querying the system, there are no records of suspended claims." It also indicated "[t]here were no written policies in place during the [C]omplaint [P]eriod."[3]

[11] Having reviewed the records received from Physician and HSS's response, I was not satisfied with HSS's assertion that it does not have any records to produce in response to my request for production of records as above-noted. Consequently, I determined it was necessary to convene an oral hearing as part of my Consideration so that I could directly question the witnesses about these records and the search undertaken in respect of them. I instructed the Registrar to arrange for an oral hearing and to compel several of IHHS's employees, including the Director and the Manager in charge of physician claims, to appear before me to give sworn testimony.

[12] The oral hearing began on January 15, 2018 and ended February 19, 2018. After its conclusion, the Complainant and Custodian had until March 15, 2018 to make submissions in respect of the testimony given by the employees. The period for submissions ended on March 15, 2018. Only the Complainant provided a response. The response was comprised of his observations and conclusion drawn during the oral hearing.

III JURISDICTION

[13] The definition of "custodian" in HIPMA includes "the Department." "Department" is defined as "the Department of Health and Social Services." Subsection 7 (1) states that "[e]xcept as provided in subsection (2), this Act applies to (a) the collection, use and disclosure of personal health information by (i) …the Department." Subsection 19 (1) further identifies that "[a] custodian must protect personal health information by applying information practices that include administrative policies and technical and physical

---

[3] Letter from S. Samis, Deputy Minister of the Department of Health and Social Services, November 10, 2017.

safeguards that ensure the confidentiality, security, and integrity of the personal health information in its custody or control."

[14] In the Fact Report agreed to by the parties, HSS acknowledges that it is a custodian as defined in HIPMA and that the information collected by it qualifies as personal health information as defined in HIPMA. I agree that HSS is a custodian and that the information collected by it for the purposes of remunerating Physician is personal health information and I find the same.

IV ISSUES

[15] The two issues for consideration identified in the Notice of Consideration are as follows.

1. *Is the* [Custodian's] *collection and use of personal health information from Physician patient files for the purpose of remunerating Physician for services rendered authorized under HIPMA?*
2. *Do the measures in place to protect the security of the personal health information collected by* [Custodian] *from Physician that is in* [Custodian's] *custody and control meet the requirements of HIPMA?*

(Complaints)

[16] Issue 1 references the location of the collection and use of personal health information by the Custodian as "from Physician patient files." The location from which personal health information is collected is not relevant to this Consideration. Evaluating the location would only be relevant in the context of evaluating Physician's information management practices as a custodian under HIPMA. The focus of this Consideration is not on Physician. As such, I will not address this aspect of Issue 1.

V BURDEN OF PROOF

[17] Section 106 establishes the burden of proof for a Consideration. Paragraph 106 (1)(b) states as follows.

106 (1) In the consideration of a complaint under this Act

(b) it is up to the respondent to prove they have acted in accordance with this Act and, if the review relates to their exercise of any discretion under this Act, that they exercised the discretion in good faith.

[18] Given that the Complaint is about the Custodian's obligations to comply with HIPMA for the collection, use and security of personal health information, it has the burden of proving that it met these obligations.

VI RECORDS AT ISSUE

[19] There are no records at issue in this Consideration since the issues are about the collection, use and security of records containing personal health information rather than access to these records.

VII FACTS

[20] The facts agreed to by the parties relevant to the issues are as follows.

1. *On November 28, 2016, the Complainant made a complaint to the* [IPC] *under section 99(1) of* [HIPMA].
2. *On December 8, 2016, the IPC notified the Custodian of the complaint as required by section 100 of HIPMA.*
3. *This Consideration arises from a complaint that the* [Custodian's] *collection and use of personal health information contained in* [Physician] *patient files for the purpose of remunerating the physician for medical services rendered is contrary to HIPMA. The Complainant also complained about the lack of security measures in place to protect the personal health information collected by the* [Custodian] *from Physician that is in* [Custodian's] *custody or control.*
4. *The IPC assigned an investigator to attempt an informal settlement of the complaint.*
5. *On February 2, 2017 the investigator advised the IPC that attempts to settle the complaint were not successful in resolving the complaint.*
6. *The* [Custodian] *is a "custodian" under HIPMA.*

7. *The information collected by the* [Custodian] *qualifies as "personal health information" as defined under the HIPMA.*

ISSUE 1: Is the* [Custodian's] *collection and use of personal health information from Physician patient files for the purpose of remunerating Physician for services rendered authorized under HIPMA?

Custodian's Initial Submission for Issue 1

[21] The Custodian's submission for Issue 1 is as follows.

1. *Personal health information (PHI) is lawfully collected from physician patient files by the* [Custodian].
2. *To presuppose as does the complainant in setting out his complaint as defined above in Issue 1, that such collection and use is done solely for the purpose of remunerating physicians, is to misstate the purposes of such collection and use. Remuneration of physicians is only one of the lawful reasons why the* [Custodian] *occasionally collects and uses PHI from physician patient files.*
3. *Insured Health and Hearing Services (IHHS) is the part of the Department of Health and Social Services (HSS) that occasionally collects and uses PHI from physician patient files.*
4. *IHHS is managed by a Director (the Director), who reports to an Assistant Deputy Minister, and ultimately to the Deputy Head of HSS.*
5. *The Director has a number of staff who report to her, and who are employed by Government of Yukon for the purpose of assisting the Director in performing her duties under various Acts.*
6. *Collection of PHI is authorized under s. 53 of the HIPMA if such collection is authorized by law (s. 53 (b)), or if such collection relates to and is necessary for carrying out a program or activity of the public body (s. 53 (c)).*
7. *Indirect collection of PHI (from the physicians rather than from the patient) is authorized under s. 54 (c)(i) of HIPMA, provided that "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 purpose without the individual's consent.*

8. *Section 56 (1)(b) provides that "A custodian may, without an individual's consent, use the individual's personal health information that is in its custody or control…subject to the requirements and restrictions, if any, that are prescribed, if an enactment of Yukon or Canada, or a treaty, arrangement or agreement entered into under such an enactment, permits or requires the use."*

9. *The Director is the director of the Yukon Health Care Insurance Plan appointed per s. 4 of the Health Care Insurance Plan Act, RSY 2002, c. 107 (HCIPA).*

10. *The Director is given various powers under s. 5 of the HCIPA. Those powers include:*

    a. *administering the Yukon Health Care Insurance Plan (the Plan) as the chief executive officer of the Plan;*

    b. *establishing advisory committees and appointing individuals to assist or advice in the operation of the plan;*

    c. *establishing what information is required to be provided to her under the HCIPA and establishing what form that information must take; and*

    d. *appointing inspectors and auditors to examine and obtain information from medical records, reports and accounts.*

11. *It is an offence under the HCIPA for any person to obstruct or hinder an inspector or auditor in carrying out duties or functions under the Act or the regulations (s. 15 (3)).*

12. *Section 27 of the HCIPA provides:*

    27 (1) An inspector may, for the purpose of enforcing this Act or the regulations,

    (a) inspect and examine all books, payrolls, and other records of an employer that in any way relate to the remittance of premiums by the employer to the director;

    (b) inspect, examine, and audit books, accounts, reports, and medical records of medical practitioners, dentists, health care practitioners, and other persons to whom amounts in respect of health services may be paid, respecting the performance or supply of insured health services;

(c) take extracts from or make copies of any entry in the books, payrolls, and other records mentioned in paragraphs (a) and (b);

(d) require any employer to make or supply full and correct statements, either orally or in writing in the required form, respecting the collection and remittance of premiums; and

(e) at any reasonable time, enter on any place used in connection with any business establishment for the purpose of making an inspection under this section.

13. *Under s. 7 of the Regulations Respecting Health Care Insurance Services, OIC 1971/275, as amended (the Regulations), a medical practitioner seeking to get paid under the Plan must "submit his claim for the services to the Administrator together with such information as is required to substantiate it, upon prescribed terms".*

14. *And under s. 8 of the Regulations, the Director is given the power "to require and receive any and all information that he considers necessary in order to adjudge the claims for services rendered to insured persons by medical practitioners."*

15. *S. 54 (c)(i) of the HIPMA applies to permit indirect collection by the Director of PHI from the physician and s. 56 (1)(b) of the HIPMA applies to permit the use of such PHI by the Director, as an enactment of Yukon (HCIPA and the Regulation) permits or requires such use.*

16. *Accordingly there is statutory authority given under the HCIPA and Regulations to the Director to indirectly collect, and use PHI in the form of extracts from physician patient files "for the purpose of remunerating physicians for medical services rendered."*

17. *That should suffice to address the complaint as set out in Issue 1. We note in that regard that the idea that a third payor for services is entitled to audit the performance of the services that it is being asked to pay for is hardly unique to the Plan.*

18. *We also point out that there is a duty imposed on the Directors, as there is on every member of the public service, to safeguard public money by properly verifying that amounts claimed from the government are properly payable by the government – see ss. 29 and 30 of the Financial Administration Act (FAA) in that regard.*

19. *In particular, by s. 29(1) of the FAA, no payment can be made to any physician unless somebody in the Director's office signs a certificate confirming, among other things, "that all conditions precedent to the making of the payment have been met" (s. 29 (2)(c)). Obviously that requires that the person signing on account of a physician's claims for payment must be satisfied that the physician has properly supplied the services being billed for.*

20. *Further, by s. 30 of the FAA no actual payment to a physician can be made unless another person signs a request for payment that, among, other things, confirms that "the payment can lawfully be made from the vote or fund" (s. 30 (2)(a)) – which again pre-supposes among other things that the physician has properly supplied the services now being paid for.*

21. *The Director, as chief executive officer of the Plan, has a specific duty in respect of payments made under the Plan to ensure that same are made in accordance with the law. Note that it is an offence under s. 77 of the FAA for a public officer to sign a false certificate under ss. 29 or 30 of the FAA.*

22. *And of course, for a physician to knowingly submit a false billing to the plan is an offence under the HCIPA, as well as under the Criminal Code.*

23. *Although not often mentioned or prosecuted, physician fraud does occur. The Vancouver Sun recently reported (February 1, 2017, Pamela Fayerman – "B.C. urologist to plead guilty to fraud over improper billing") that a urologist in Burnaby, BC intends to plead guilty in relation to one count of criminal fraud over $5,000 on account of over billing.*

24. *That same article, citing a 2005 report prepared for the Law Commission of Canada by Simon Fraser University criminology professor Joan Broackman, reports that health care fraud, mostly by doctors, was estimated at $10 billion a year across Canada when that report was done.*

25. *Payments to Yukon physicians under the Plan amounted by $27.447 million in 2015-16.*

26. *S. 56 (1)(o) (together with s. 54 (c)(i)) allows for the indirect collection and use by the Director of PHI, including patient records, "for the purpose of (i) assisting in the prevention, detection or investigation of fraud in relation to health care, or (ii) preventing or reducing abuse in the use of health care."*

27. *Even absent cases of fraud where a physician knowingly submits a false billing, there is still a duty imposed on the Director and her staff under the FAA to detect cases where a physician innocently bills the Plan incorrectly.*

28. *To the extent that the complainant may wish to argue that it is an over-collection of PHI contrary to s. 16 of the HIPMA for the Director to require extracts from physician patient records from time to time, we submit that s. 17 of the HIPMA applies to this situation.*

29. *That section states:*

 17 Section 13, 15 and 16 do not apply to the extent that a law, including an order of a court or other order that has the force of law, requires the collection, use or disclosure of, or access to, personal health information.

30. *In our view, the combination of the powers given to the Director under the HCIPA and the Regulations, together with the duty imposed on her under the FAA, is such that a law requires the collection and use of personal health information for the purpose of verifying physician billings.*

31. *That means that the rules that:*

 a. *PHI can only be collected, used and accessed in accordance with the HIPMA and regulations under (s. 13);*

 b. *PHI should not be collected or used if other information will serve the purpose of such collections or use (s. 15);*

 c. *PHI should only be collected and used to the minimum amount reasonably necessary to achieve the purpose for which it is collected and used (s. 16);*

 do not apply to the collection and use of PHI by the Director for the purpose of administering the HCIPA and Regulations.

32. *Notwithstanding the above proposition, the Director nonetheless recognizes the principles found in ss. 13, 15 and 16 of the HIPMA as having moral, if not legal, force in terms of how she administers the HCIPA and Regulations. For that reason, her office is engaged in the on-going development and refinement of policies for her staff to follow in administering the HCIPA and Regulations aimed at minimizing the collection of patient PHI while maximizing the ability of her staff to detect incorrect billings.*

[22] The Custodian provided an Affidavit sworn by the Director in support of the submissions with the following exhibits attached:

a. Exhibit A is an article printed from the Internet dated February 1, 2017 and titled "B.C. urologist to plead guilty to fraud over improper billing;"

b. Exhibit B is a memorandum issued by the Director of IHHS to "All Yukon Physicians," dated December 14, 2016 with a subject line that states "Physician Claim Review/Audit Policy Manual;"

c. Exhibit C is the "Yukon Insured Health and Hearing Services Physician Claim Review/Audit Policy Manual January 1, 2017;"

d. Exhibit D is a policy of the Custodian specific to IHHS titled "Removable Media and Laptops" dated January 9, 2017;

e. Exhibit E is a policy of the Custodian specific to IHHS titled "Clean Desk Policy" dated January 9, 2017; and

f. Exhibit F is a policy of the Custodian specific to IHHS titled "General Office Workplace Security Policy" dated January 9, 2017.

<u>Complainant's Initial Submission for Issue 1</u>

[23] The Complainant's initial submission on Issue 1 is as follows.

> "*My original complaint and concerns where [sic] based on conversations with* [Physician] *and myself…*[Physician] *informed me that the department of Health and Social Services had and continued to request full patient files from him to verify billing. [Physician] could not confirm who in the department would be looking at the files and what if any security/confidentiality would or could be maintained outside of his office.*

[24] The Complainant then went on to say that the contents of his medical records with Physician contains highly sensitive personal health information that he did not want "anyone else to see." He added that it was unclear to him if the Custodian has adequate security measures in place to protect the personal health information it collects.

Custodian's Reply Submission for Issue 1

[25] In its reply, the Custodian stated the following.

…

The complainant also questioned the "Government's Guidelines for the transmittal of confidential, secret, or, better information?" and requested what level of security does HSS place of individual medical records, confidential, confidential A, confidential B…?

This response does not address the Government's Guidelines nor overall HSS policies but will address the concerns raised in the letter regarding Insured Health and Hearing Services Branch (IHS) policies.

Policies and procedures in place with IHS regarding the complainant's questions and concerns:

- *On January 1st* [2017] *a new policy was put in place and listed on the Yukon Physician Pages web page "Physician Claim Review/Audit Policy Manual". This policy deals with the minimum information required to substantiate a claim. IHS is working with physicians to advise them of this policy and returning information to the physician if not required or advising them on where to redact information not required for the audit;*

- *IHS has implemented three internal policies for all IHS staff to ensure the security of the information held in office: 2016-B0001 Clean Desk Policy, 2016-B0002 General Office Workplace Security Policy and 2016-B0003 Removable Media and Laptops. In addition to these policies, IHS also instituted a policy where all visitors must sign in at the office, be issued a visitor's pass and then sign out of the office to further enhance security; and,*

- *IHS faxes are received and sent via YNET to a group inbox with access to only IHS staff and contractors who work in the office and are under Confidentiality Agreements and have taken HIPMA training. IHS is working with the Departments* [sic] *internal Information Technology Department to further secure faxes by reducing access to the primary inbox to three staff members who will then move the faxes to individually secured inboxes for each of the program areas at IHS. These individual inboxes will only be able to be accessed by program staff for each area and the three individuals responsible for*

redirecting mail sent to the general IHS inbox. It is anticipated these changes will be in place by the end of March 2017.

[26] The Complainant did not provide a reply submission.

VIII ANALYSIS

Section 17

[27] I will begin my analysis by determining if section 17 applies to the collection and use of personal health information by the Custodian in respect of Issue 1.

[28] The Custodian submitted that through a combination of the powers of the Director under the HCIPA, HCIPR and the *Financial Administration Act* (FAA),[4] section 17 applies to the personal health information that it collects and uses under the HCIPA and HCIPR. Its position is that because this section applies, sections 13, 15 and 16 “do not apply to the collection and use of [personal health information] by the Director for the purpose of administering the HCIPA and [HCIPR].”

[29] It also submitted the following in respect of the interpretation of sections 17 and 13.

a. The term “‘requires’” is “critical to understanding the meaning of s. 17.”

b. Section 13 “clearly limits the collection, use, disclosure of, and access to, personal health information to what is permitted by the HIPMA and regulations made under it.”

c. The word “‘may’ in section 13 is an expression of limitation; it is not used in its permissive, or power granting, sense.”

d. “…where s.17 applies, that limitation on how one may collect, use, disclose and access personal health information does not apply.”

e. “…where s.17 applies, on the plain language of that section and s.13, a person who is a custodian or the agent of a custodian may collect, use, disclose and access personal health information in accordance with what the order or other law requires.”

[4] RSY 2002, c 87.

f. "…s.17 and s.13 together provide a method for custodians or agents of custodians to comply with the law – by acting as the law (or order) requires, notwithstanding any restrictions that might be found in HIPMA."

g. "…A necessary condition for section 17 to operate is the existence of a law or order that requires a collection, use, disclosure, or access."

h. Subsection 53 (b) which allows for collection of personal health information where doing so is "authorized by law" is not equivalent to section 17 "which deals with circumstances where the law 'requires' collection..."

i. "We do agree that section 17 exempts a custodian's actions as it relates to the collection, use or disclose [sic] of personal health information only if a court or other order, or law, 'requires' the collection, use or disclosure. We also agree that "the custodian would have to point to some law that requires it".

j. "We point out that we have pointed to a law, namely the [FAA] that requires the director, as a public official, to expend public money only for the purposes for which it was appropriated."

[30] I will undertake a purposive analysis of section 17 in order to determine how this provision is to be interpreted.

[31] The modern approach to statutory interpretation is that the words of an Act are to be read in their entire context and in their grammatical and ordinary sense harmoniously with the scheme of the Act, the object of the Act, and the intention of Parliament.[5]

[32] In Yukon's *Interpretation Act*[6], it states "[e]very enactment and every provision thereof shall be deemed remedial and shall be given the fair, large, and liberal interpretation that best insures the attainment of its objects."

[33] The purposes of HIPMA are set out in section 1 as follows.

1 The purposes of this Act are

[5] *Rizzo & Rizzo Shoes Ltd. (Re)*, [1998] 1 SCR 27, 1998 CanLII 837 (SCC), at para. 21.

[6] RSY 2002, c 125, section 10.

(a) to establish strong and effective mechanisms to protect the privacy of individuals with respect to their health information and to protect the confidentiality of that information;

(b) to establish rules for the collection, use and disclosure of, and access to, personal health information that protect its confidentiality, privacy, integrity and security, while facilitating the effective provision of health care;

(c) subject to the limited and specific exceptions set out in this Act, to provide individuals with a right of access to their personal health information and a right to request the correction or annotation of their personal health information;

(d) to improve the quality and accessibility of health care in Yukon by facilitating the management of personal health information and enabling the establishment of an electronic health information network;

(e) to provide for an independent source of advice and recommendations in respect of personal health information practices, and for the resolution of complaints in respect of the operation of this Act; and

(f) to provide effective remedies for contraventions of this Act.

[34] In my decision issued about my jurisdiction to consider the Complaint, I stated the following about the context in which the provisions in HIPMA must be interpreted.

The protection of personal information privacy has been recognized by our highest court to be quasi-constitutional in nature. The SCC in Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401 stated that "[t]he importance of protection of privacy in a vibrant democracy cannot be overstated." Personal health information goes to the biographical core of individuals. Therefore, it is the most sensitive personal information that exists. Health information laws were developed to facilitate the flow of personal health information to provide individuals with healthcare and to effectively manage Canada's public health system while taking into account that the information collected, used and disclosed by custodians for these purposes is the most sensitive type that, if breached, could result in significant harm to individuals.

HIPMA is no exception. It is clear from the purposes in HIPMA that the drafters recognized that to facilitate the flow of personal health information for health care

and health system management, strong controls and accountability mechanisms are necessary to maximize privacy and security and minimize the risk of harm…[7]

[35] I also stated the following about HIPMA's scheme.

HIPMA applies to custodians. The term "custodian" is defined in section 2 to include the Department of Health and Social Services (HSS)…, the operator of a hospital or health facility, a health care provider, a prescribed branch, operation or program of a Yukon First Nation, and the Minister of HSS. Essentially, custodians are those persons or bodies in Yukon who engage in the provision of health care or who have responsibility for management of the health system.

Section 6 indicates that the Yukon Government (YG) is bound by it. HSS is a YG department.

Section 7 of HIPMA sets out that it applies to the collection, use and disclosure of personal health information by the Minister, HSS or "any other custodian, if the collection, use or disclosure is undertaken for the purpose of providing health care, the planning and management of the health system or research."

Section 11 specifies that HIPMA prevails over an Act or regulation, the provisions of which, conflict with those in HIPMA unless expressly stated otherwise.

[36] I also stated that HIPMA is a complete governance scheme for the collection, use, disclosure and management of personal health information by custodians.[8]

[37] Section 17 states as follows.

17 Sections 13, 15 and 16 do not apply to the extent that a law, including an order of a court or other order that has the force of law, requires the collection, use or disclosure of, or access to, personal health information.

[38] Sections 13, 15 and 16 state as follows.

13 A person who is a custodian or the agent of a custodian may collect, use, disclose and access personal health information only in accordance with this Act and the regulations.

[7] HIP16-02I Decision, Department of Health and Social Services, October 6, 2017 (YT IPC) at paras. 52 and 53.

[8] HIP16-02I Decision, Department of Health and Social Services, October 6, 2017 (YT IPC) at para. 75.

> *15 A person who is a custodian or the agent of a custodian must not collect, use or disclose personal health information if other information will serve the purpose of the collection, use or disclosure.*

> *16 The collection, use and disclosure of personal health information by a custodian or their agent must be limited to the minimum amount of personal health information that is reasonably necessary to achieve the purpose for which it is collected, used or disclosed.*

[39] Section 14 is also relevant to the interpretation of the limitation provisions in Division 1 of Part 3. It states as follows.

> *14 Nothing in this Act limits any person's right to collect, use or disclose information that is not identifying information.*

[40] I agree with the Custodian that the term "requires" is critical to understanding the meaning of section 17. I disagree, however with its interpretation of section 13 and how this provision works with sections 14, 15, 16 and 17. These sections must all be read together and their interpretation in accordance with the object and scheme of HIPMA and the intent of the Legislature. As stated previously, HIPMA is a complete governance scheme for the collection, use, disclosure and management of personal health information by custodians. This means that custodians are only allowed to collect, use, disclose and manage personal health information in accordance with its requirements. There are no other circumstances that allow a custodian to collect, use, disclose or access personal health information except those set out in section 17, which I will discuss below.

[41] The purpose of section 13 in this context is to establish authority for custodians to collect, use, disclose or access personal health information by clarifying that they are authorized to do so "only" in accordance with the rules set out in HIPMA. The "may" in section 13 is permissive[9] thereby establishing the authorization or "power" of custodians to collect, use, disclose or access personal health information. The word "only" appears after the words "collect, use, disclose and access personal health information" and before "in accordance with this Act and the regulations." This placement signals to the reader that if a custodian chooses to exercise its authority to collect, use or disclose personal health information, then its only option is to follow the rules set out in HIPMA.

---

[9] This is consistent with subsection 5 (3) of the *Interpretation Act*, RSY 2002 c 125, which states that "[t]he expression "shall" shall be read as imperative and the expression "may", as permissive and empowering.

[42] After a custodian determines that it has authority to collect, use, disclose or access personal health information within HIPMA's provisions, it must turn its mind to the requirements in sections 15 and 16. These sections restrict the amount of personal health information that a custodian may collect, use or disclose to that which, essentially, is necessary to achieve the purpose of the collection, use or disclosure while recognizing, in section 14, that custodians are not restricted in these activities when it comes to information that is non-identifying or not "personal health information."[10] The limitations in these provisions are consistent with the purposes of HIPMA in subsections 1 (a) and (b).

[43] Given that custodians are bound to follow the rules in HIPMA for any collection, use, disclosure and access to personal health information, section 17 operates as a means to allow a custodian to comply with a law, other than HIPMA, that "requires" the custodian to collect, use, disclose or access personal health information for purposes other than health care or health system management.

[44] As a complete governance scheme over the collection, use, disclosure and management of personal health information by custodians, HIPMA's provisions were carefully crafted to facilitate the flow of personal health information for the provision of health care in Yukon and for management of its public health care system. The purposes in HIPMA support that these activities may only occur where the privacy and security of personal health information collected, used, disclosed or accessed by custodians are maximized through compliance with HIPMA's provisions. Custodians are bound by HIPMA's provisions and must comply with them when undertaking these activities. Given this, the meaning of "law" which is used a number of places in HIPMA, must mean a law other than HIPMA that exists for some purpose extraneous to the delivery of health care or health system management.

[45] Section 17 establishes when a custodian may collect, use, disclose or access personal health information; *i.e.*, when a law requires it. It also establishes the amount of personal health information a custodian may collect, use or disclose; *i.e.*, "<u>to the extent that</u> a law… requires it." The limitations built into this provision also support the purposes of subsections 1 (a) and (b).

[46] The Custodian takes the position that section 17 applies to its collection and use of personal health information under the HCIPA and HCIPR. It submissions on this point are that the "combination of the powers given to the Director under the HCIPA and HCIPR, together

[10] Section 14 states "Nothing in this Act limits any person's right to collect, use, or disclose information that is not identifying information."

with the duty imposed on her under the [*Financial Administration Act* (FAA)[11]], is such that a law requires the collection and use of personal health information for the purpose of verifying physician billings. It added its view that section 17 applies to this collection and use because the FAA requires the Director, as a public official, to expend public money according to FAA's requirements. I disagree with the Custodian that section 17 applies to this collection and use of personal health information by the Custodian.

[47] While I accept that the HCIPA, HCIPR and the FAA are laws for the purpose of section 17, I do not accept that the HCIPA, HCIPR or the FAA on their own or in combination "require" the Custodian "to collect and use personal health information."

[48] The term "require" is not defined in HIPMA. However, it is defined in the Oxford Dictionary as:

> *needed; depend on for success or fulfillment; command; instruct (a person etc.); and order; insist on (an action or measure).*[12]

The meaning of "require" is such that, for section 17 to apply, the Custodian will need to establish that one or a combination of these laws command or order it to collect and use personal health information, or specify that the Custodian needs to collect and use personal health information.

HCIPA

[49] According to the Custodian, the Director of IHHS (Director) was appointed under subsection 4 (1) to be the director of the Yukon Health Care Insurance Plan. The powers of the Director set out in section 5 as follows.

> *5 Subject to this Act and the regulations, the director may*
>
> *(a) administer the plan as the chief executive officer of the plan;*
>
> *(b) determine eligibility for entitlement to insured health services;*
>
> *(c) register persons in the plan;*
>
> *(d) collect premiums;*

[11] RSY 2002, c 87.

[12] Canadian Oxford Dictionary, Second Edition, edited by Katherine Barber, Don Mills Ontario, 2004.

(e) make payments under the plan, including the determination of eligibility and amounts;

(f) determine the amounts payable for insured health services outside the Yukon;

(g) establish advisory committees and appoint individuals to advise or assist in the operation of the plan;

(h) conduct actions and negotiate settlements in the exercise of the Government of the Yukon's right of subrogation under this Act to the rights of insured persons;

(i) conduct surveys and research programs and obtain statistics for those purposes;

(j) establish what information is required to be provided to the director under this Act and the form that information must take;

(k) appoint inspectors and auditors to examine and obtain information from medical records, reports, and accounts; and

(l) perform any other functions and discharge any other duties assigned to the director by the Minister under this Act.

[50] The Director is authorized under subsection 5 (k) (above) to appoint inspectors. "Inspector" means a person appointed pursuant to subsection 4 (2) or paragraph 5 (k). The authority of inspectors is set out in subsection 27 (1) of the HCIPA and states as follows.

27(1) An inspector may, for the purpose of enforcing this Act or the regulations,

(a) inspect and examine all books, payrolls, and other records of an employer that in any way relate to the remittance of premiums by the employer to the director;

(b) inspect, examine, and audit books, accounts, reports, and medical records of medical practitioners, dentists, health care practitioners, and other persons to whom amounts in respect of health services may be paid, respecting the performance or supply of insured health services;

(c) take extracts from or make copies of any entry in the books, payrolls, and other records mentioned in paragraphs (a) and (b);

(d) require any employer to make or supply full and correct statements, either orally or in writing in the required form, respecting the collection and remittance of premiums; and

(e) at any reasonable time, enter on any place used in connection with any business establishment for the purpose of making an inspection under this section.

<u>HCIPR</u>

[51] The relevant portions of the HCIPR are below.

7. (1) Where a medical practitioner renders an insured service to an insured person, he shall, unless he has made an election pursuant to this section, submit his claim for the service to the Administrator together with such information as is required to substantiate it, upon prescribed terms, and, subject to these Regulations, payment shall be made to the medical practitioner under subsection (2) without undue delay, except, where a notice pursuant to subsection (3) of section 12 has been sent to the medical practitioner or his professional association by either the Administrator or the medical practitioner or where the professional association of a medical practitioner requests otherwise.

8. The Administrator shall have the power to require and receive any and all information that he considers necessary in order to adjudge the claims for services rendered to insured persons by medical practitioners.

[52] The HCIPA does not command or order the Custodian, through the Director or otherwise, to collect and use personal health information for the purposes of the HCIPA. Nor does it specify that that the Custodian needs to collect or use personal health information for these purposes. What the HCIPA does in section 5 is "permit" the Director to determine the information she needs in order to carry out her obligations. She is also permitted under section 5 to appoint an inspector. Under subsection 27 (1), the inspector is permitted to obtain information from records, including personal health information from physician's medical records, for the purposes of inspection. The use of the word "may" in those provisions mean that there is no requirement for the Director or inspector to collect and use personal health information for the purposes of the HCIPA and that the decision to do so is at their discretion.

[53] In the HCIPR, the Director is granted the power, as administrator of the Yukon Health Care Insurance Plan, to "require and receive any and all information that [she] considers necessary in order to adjudge the claims for services rendered to insured persons by medical practitioner." Since the exercise of the Director's power in this regard is at her discretion, the HCIPR does not require her to collect and use personal health information for those purposes identified in this section.

[54] The FAA governs the receipt and management of "public money."[13] The FAA establishes the structure required to manage public money and imposes obligations on public servants who receive or manage public money, including, as the Custodian pointed out in its submissions, the Director responsible for managing the public money flowing in and out of the Yukon Health Care Insurance Plan. While it may be that the Director decides to collect and use personal health information to substantiate billing claims made by Physician in order to meet her obligations under the FAA, which she is 'permitted' to do under the HCIPA, there is nothing in the FAA that 'requires' her or the Custodian to do so.

[55] My conclusions in regards to the application of section 17 to the personal health information collected and used by the Custodian under the HCIPA and HCIPR are supported by HIPMA's scheme, object and the intent of the Legislature.

[56] The Custodian's position that section 17 applies to its collection and use (and disclosure and access for that matter) of personal health information under the HCIPA and HCIPR is untenable in the context of HIPMA's purposes.

[57] When the legislation was drafted, it is reasonable to expect that all relevant aspects of health care delivery and system management known at the time were considered and captured within HIPMA's provisions. The Yukon Health Care Insurance Plan is a fundamental component of this system. Given this, had the drafters intended that personal health information collected, used, disclosed or accessed under the HCIPA and HCIPR were to operate outside the HIPMA, then the legislation would state this clearly as an exemption under subsection 7 (2). Subparagraph 7(1)(a)(i) instead clarifies that HIPMA applies to "the collection, use and disclosure of personal health information by…the Department." This provision is an unambiguous expression of the Legislature's intent about the application of HIPMA to the Custodian and its collection and use of personal health information under the HCIPA and HCIPR.

[58] HIPMA's provisions are very detailed such that nearly every aspect of health care delivery and management is addressed to facilitate the flow of personal health information within and between custodians for these purposes. As the Custodian pointed out in its submissions, there are several provisions in HIPMA that authorize the Custodian to collect and use personal health information for the purposes of the HCIPA and HCIPR, including support for the effective management of the Yukon Health Care Insurance Plan.

---

[13] "Public money" is defined in subsection 1 (1) of the FAA as "all money and negotiable instruments received, held, or collected by, for or on behalf of the government…"

[59] Taken together, it is clear that the legislature intended the collection, use, disclosure and access of personal health information for the purposes of the HCIPA and HCIPR by the Custodian to be subject to the rules in HIPMA governing collection, use, disclosure and access to personal health information, including those rules in sections 15 and 16. In my view, the purposes of HIPMA would be undermined if the very controls established by HIPMA designed to maximize security and protection of personal health information, while facilitating the flow of personal health information for health care and health system management, did not apply to the Custodian who is responsible for the management of Yukon's publicly-funded health care insurance.

[60] Based on the foregoing, I find that section 17 does not apply to the collection and use of personal health information by the Custodian under the HCIPA, HCIPR or the FAA, or combination thereof, for the purpose of remunerating Physician.

[61] Section 13, as noted above, requires the Custodian to comply with HIPMA and its regulations for the collection and use of personal health information, including the collection and use of personal health information for remunerating Physician. Given this, I will now go on to consider if the Custodian has authority under HIPMA's other provisions to collect and use personal health information for remunerating Physician.

Collection of personal health information

[62] Part of issue 1 is whether the Custodian's "collection" of personal health information from Physician patient files for the purpose of remunerating Physician for services rendered is authorized under HIPMA.

[63] "Collect" is defined in HIPMA as "to gather, acquire, receive or obtain by any means from any source, but does not include the transmission of information between a custodian and an agent of that custodian." The term "collection" is not defined but the Oxford Dictionary defined it as "the action or process of collecting or being collected."[14]

[64] For the Custodian to have collected personal health information, it would need to have gathered it, acquired it, received it or obtained it from an external source. For its collection, however, the Custodian would need to have undertaken some action or process to collect the personal health information.

---

[14] Canadian Oxford Dictionary, Second Edition, edited by Katherine Barber, Don Mills Ontario, 2004.

Did the Custodian collect personal health information from Physician?

[65] As indicated above, the Custodian's written submissions were that it had no records containing personal health information collected from Physician. On my request, Physician produced records that listed 200 billing claims he submitted via his electronic medical record system (EMR) to IHHS on or between August 31, 2016 and November 28, 2016 (the Complaint Period).

[66] During the oral hearing, I received evidence from Physician's Office Manager that these billing claims were submitted and processed by IHHS through a combination of its E-billing System and a manual process.[15] A Manager within IHHS confirmed that these billing claims were received by IHHS, processed for payment, and that the personal health information collected by IHHS for the purposes of processing Physician's billing claims is maintained in its electronic physician billing claims processing system (E-billing System).[16]

[67] Based on written evidence submitted by the Custodian, the personal health information processed by the E-billing System is "retained indefinitely."[17] Another Manager of the Custodian confirmed that this information "would still be in the [E-billing System]."[18]

[68] The information that the Custodian collected from Physician to process his billing claims submitted during the Complaint Period is as follows.[19]

a. claim# (auto generated by the system);

b. Physician's billing number;

c. service date and time;

d. number of services;

e. patient name;

---

[15] Physician Office Manager, at p.10 of the transcript, at lines 14 to 17.

[16] Manager, Registration, Medical Travel and Hospital and Physician Claims, at p. 59 of the transcript, at lines 1 to 23.

[17] Page 122 of the E-billing System PIA, section 8.3.3.

[18] Manager, Health Informatics and Information Technology (who also had other roles in IHHS during the investigation including Acting Director, IHHS, at p. 29 of the transcript, at lines 21 to 25.

[19] There was additional information on the records, such as "doctor code", the meaning of which could not be verified by the witnesses.

f. name of family member or other third party when counselling involves these individuals;

g. amount billed;

h. billing code (also referred to as a "fee code");

i. referring doctor billing number (where a referral is involved); and

j. diagnosis.

[69] Evidence provided by the Custodian indicates that it also collects the patient's Yukon Health Care Insurance Plan card number (Insurance Number) and the number of times the service was received.[20]

[70] The meaning of "personal health information" in HIPMA is as follows.

> *"personal health information" of an individual means*
> *(a) health information of the individual, and*
> *(b) except as prescribed, prescribed registration information and prescribed provider registry information in respect of the individual;*
>
> *"health information" of an individual means identifying information of the individual, in unrecorded or recorded form, that*
> *(a) relates to the individual's health or the provision of health care to the individual,*
> *(b) relates to payments for health care,*
> *…*
>
> *"health care" means any activity (other than an activity that is prescribed not to be health care) that is or includes*
> *(a) any service (including any observation, examination, assessment, care, or procedure) that is provided*
> *(i) to diagnose, treat or maintain an individual's physical or mental condition,*
> *(ii) to prevent disease or injury or to promote health,*

[20] This personal health information collected by the Custodian to process Physician billing claims was identified through the records produced by Physician (Plexia report and YHCIP Aging Report) and verified by an IHHS employee during the oral hearing (Physician Claims Assessor, at pages 8 to 13 of the transcript) and the E-billing System PIA p. 74, as well as the suspended claim report that is generated by the E-billing System and produced by Physician.

…

"identifying information" of an individual means information that identifies the individual or that it is reasonable to believe could be used, either alone or with other information, to identify the individual;

[71] In the *Health Information General Regulation* (Regulation), the following information is prescribed as personal health information of an individual:

7 Personal health information of an individual includes
(a) registration information in respect of the individual; and

…

[72] The Regulation defines "registration information" to include any unique identifier assigned by a Custodian's information system to identify the individual.[21] "Provider registry information" in the Regulation includes a unique identifier that a regulatory authority related to health care has assigned the health care provider."[22]

[73] The information collected by the Custodian from Physician qualifies as personal health information for the following reasons.

a. The information identifies a patient, an individual, by name. This information, together with all the other information collected by IHHS to process a billing claim, qualifies as identifying information.

b. The unique identifier assigned by the E-billing System for the billing claim submitted by a physician for payment of the care received by the patient is registration information.

c. The information contains the patient's diagnosis, the care received by the patient as indicated by the billing or fee code, the date and time of the patient's care and the number of times the care was received, the patient's Insurance Number, the amount billed and paid under the patient's Insurance Number as well as any amount not paid. This information qualifies as health information.

[21] Regulation, section 1.

[22] Regulation, section 1.

d. Physician's and referring physician's billing number assigned to them by IHHS would also qualify as the patient's personal health information, given that it would fall within the definition of provider registry information.

[74] The evidence provided by the Custodian, together with the records (billing claims and suspended claim report or "yellow sheet"), suggests that the Custodian endeavoured to collect additional personal health information from Physician to substantiate payment for his billing claim under fee code 610.

[75] One of Physician's billing claim on the record containing his 200 billing claims is for fee code 610. During the oral hearing, Physician produced a suspended claim report that he received from IHHS in regards to this claim. On the suspended claim report there is a message that states "224-Copy of clinic record requested."

[76] During the oral hearing, I was provided the following information about what a clinic record is and the rationale for requesting a copy of a clinic record for a fee code 610 billing claim.

[77] An IHHS witness indicated that a clinic record is a record that contains information IHHS needs to verify the type of service for which Physician is billing. The witness testified that what constitutes a clinic record is derived from the Payment Schedule for Yukon, April 1, 2016 (Schedule).[23] The Schedule, an IHHS document, sets out the fees associated with codes physicians use to bill for services rendered. For fee code 610, it says the following.

> *610 Adult Consultation: Diagnostic interviews or examination, including history, mental status and treatment recommendation, with written report.*

[78] In the Schedule, fee code 610 falls under the heading "Consultations: (office, home or hospital)" and "REFERRED CASES." Above these headings are the words "These fees cannot be correctly interpreted without reference to the Preamble."

[79] At the start of the preamble to the Schedule, it states that "Complete understanding of the following paragraphs is essential to proper interpretation of the Guide." The Preamble identifies a number of different types of physician' services. For each service, an explanation is provided as to the meaning.

---

[23] According to the Preamble of the Payment Schedule, April 1, 2016 (Schedule), the fees payable by the Yukon Health Care Insurance Plan are the result of negotiation between the Yukon government and the Yukon Medical Association. See page 3 of the Schedule.

[80] For the consultation and continuing care by consultant services, it states as follows.

> *4. Consultation*
>
> *This is defined as a request by a doctor for a second opinion on a case he/she has examined and with which he/she has encountered some difficulty. It includes the initial services of a consultant and additional visits necessary to enable him/her to prepare and render his/her report. Subsequent consultations may be sought by the original doctor from the same or other consultants. No consultation should be charged to a patient or their payment agency unless it was requested by the attending doctor.*
>
> *5. Continuing Care By Consultant*
>
> *This may follow consultation at the request of the referring doctor if the complexities of the case are such that its management should remain for a time in the hands of the consultant. In such circumstances, the consultant will charge for his/her consultation and continuing care according to the Fees pertaining to his/her specialty.*
>
> *Should the referring doctor consider that continuing consultant care of his/her patient is still necessary after six months, he/she should review the case and re-refer the continuing care only… When a referral takes place, it must be made clear by the referring doctor to all concerned that the major responsibility for the case has been transferred, and the referring doctor may not charge for the case until, or unless, the full responsibility is returned to him/her, expect that for a patient in hospital, he/she may charge supporting care where the patient's condition warrants it.*

[81] The witness stated that "In order for the [Physician] to receive payment under fee code 610, as identified in the Schedule, they need to provide IHHS with a written report."[24]

[82] The witness clarified, in reference to an example letter contained in the Manual implemented by IHHS in January of 2017 to guide IHHS employees on what personal health information they may collect to process a fee code 610 billing claim,[25] that a written report consists of a letter of response written by Physician to the referring physician that contains

---

[24] Director, IHHS, at p. 30 of the transcript, at lines 20 to 21.

[25] Appendix 2(a) in the Yukon Insured Health and Hearing Services Physician Claim Review/Audit Policy Manual, January 1, 2017 (Manual), Exhibit C to the Affidavit of the Director of IHHS.

specific information about the patient receiving the services; namely, the patient's name and Insurance Number, an indication that the letter is in response to a referral, and the patient's history, mental status, and treatment recommendation.[26] The witness further clarified that, during the Complaint Period, the written reports collected from physicians were not redacted and, therefore, contained detailed medical information about patients.[27] The information in the written report qualifies as personal health information.

[83] It is clear from the suspended claim report submitted by Physician, together with the testimony of an IHHS employee, that the Custodian endeavoured to collect from him a written report that contains personal health information.

[84] Based on the foregoing, I find that the Custodian collected or endeavoured to collect the personal health information described above from Physician.

Authority to collect personal health information

[85] The rules that a custodian must follow to collect personal health information are set out in Division 2 of Part 6. Section 53 in that Division identifies the only three circumstances under which a custodian may collect personal health information. They are as follows.

> *(a) the custodian has the individual's consent and the collection is reasonably necessary for a lawful purpose;*
>
> *(b) the collection is authorized by law; or*
>
> *(c) the collection relates to and is necessary for carrying out a program or activity of a public body or a health care program or activity of a custodian that is a branch, operation or program of a Yukon First Nation.*

[86] In its written submissions, the Custodian indicated that it is relying on subsections 53 (b) and (c) as its authority to collect the personal health information.

---

[26] Director, IHHS, at pp. 30 to 31 of the transcript. Manager, Registration, Medical Travel and Hospital and Physician Claims, confirmed that sample 2 (a) is similar to the type of letter that would be requested from a physician who billed under fee code 610, at p. 26 of the transcript, lines 9 to 10 and p. 27 at lines 4 to 14.

[27] Director, IHHS, at p. 46 of the transcript, lines 3 to 20; and Manager, Registration, Medical Travel and Hospital and Physician Claims, at pp. 31 to 33 of the transcript.

Subsection 53 (b)

[87] Section 53, together with its subsection (b), states as follows.

53 A custodian may collect an individual's personal health information only if

(b) the collection is authorized by law;

Is the collection of personal health information authorized by law?

[88] The Custodian submitted that the Director has power under section 5 of the HCIPA to collect the personal health information from Physician based on her authority to administer the Yukon Health Care Insurance Plan (Plan) and establish the information required to be provided to her, as well as the form it must take. Moreover, it submitted that this authority, together with section 8 of the HCIPR, which authorizes her "to require and receive any and all information that [s]he considers necessary in order to adjudge the claims for services render to insured persons by medical practitioners," authorizes the collection.

[89] In order for the Custodian to have authority for the collection of the personal health information under subsection 53 (b), it must establish that there is a law that authorizes the collection of personal health information.

[90] I am satisfied that the HCIPA and HCIPR are both laws for the purposes of subsection 53 (b).

Is the collection of the personal health information by the Custodian authorized by the HCIPA and HCIPR?

[91] The HCIPA and HCIPR permit the Director of IHHS to determine the "information" she requires to substantiate billing claims submitted by Physician for services rendered to his patients.

[92] The Information and Privacy Commissioner for British Columbia's office (OIPC BC) has considered the meaning of subsection 26 (a) in British Columbia's *Freedom of Information and Protection of Privacy Act* (FIPPA). This subsection permits a public body to "collect personal information only if the collection of the information is expressly authorized under an Act." While subsection 53 (b) does not have a requirement that an Act expressly authorize the collection, it is useful to examine these decisions in the context of interpreting this subsection.

[93] In British Columbia (Justice) (Re), 2014 BCIPC 29 (CanLII), Adjudicator Barker reviewed prior decisions of the OIPC BC that considered the meaning of "expressly authorized." In doing so, she stated the following (at paras 20 to 25).

> *26 A public body may collect personal information only if*
> *(a) the collection of the information is expressly authorized under an Act*
>
> *The Commissioner has discussed s. 26(a) and what is required in order to establish that the collection of personal information is expressly authorized under an Act, at length, on four previous occasions.*
>
> *In Insurance Corp. of British Columbia, the Commissioner's delegate examined the Insurance Corporation of British Columbia's ("ICBC") collection of weight information from drivers' licence applicants. He found that this collection of personal information, in order to put it on a licence document that can be used to identify the licence holder as someone who is authorized to drive a motor vehicle, was expressly authorized by s. 25(2.1) of the Motor Vehicle Act. Section 25(2.1) states, "For the purposes of making an application for a driver's licence under subsection (1), the Insurance Corporation of British Columbia may require the applicant for a driver's licence and for a driver's certificate to provide information...".*
>
> *Investigation Report F11-03[13] dealt with BC Hydro's use of smart meters to collect hourly information about its customers' electricity consumption, information which the Commissioner determined was the personal information of BC Hydro's customers. The Commissioner concluded that s. 2(d) of the Smart Meters and Smart Grid Regulation of the Clean Energy Act, which provides that smart meters must be capable of recording measurements of electricity "at least as frequently as in 60-minute intervals", provides the express statutory authority under s. 26(a) of FIPPA for the collection of hourly electricity consumption data.*
>
> *In Investigation Report F12-01, the Commissioner examined ICBC's collection of digital photographs and biometric data, (i.e., measurements taken of an individual's facial geometry and skin texture), which she determined was personal information. The Commissioner concluded that s. 25(3) of the Motor Vehicle Act gives ICBC the express statutory authority to collect this personal information. Section 25(3) states, "For the purpose of determining an applicant's driving experience, driving skills, qualifications, fitness and ability to drive... the applicant must... (d) submit to having his or her picture taken".*

> *Conversely, in Order F07-10[15] the Commissioner found that the Mission School District's board of education did not have express statutory authorization to collect the personal information it was obliging prospective employees to provide by way of an on-line computer-based assessment tool. The board submitted that s. 15(1) of the School Act provided the express statutory authority for such collection because it charged school boards with the responsibility for hiring staff. The Commissioner, however, found that there was no language in the School Act expressly authorizing or directing the collection of personal information for the hiring process. Section 15(1) of the School Act simply says that a "board may employ and is responsible for the management of those persons that the board considers necessary for the conduct of its operations". While it was implicit that personal information would have to be collected, the Commissioner found this did not meet the requirements of s. 26(a).*

[94] What is useful from this decision, as it relates to the meaning of subsection 53 (b), is that the decisions referred by the adjudicator identify that it is enough for a law (or in the case of FIPPA an "Act") to authorize a public body under subsection 26 (a) to collect the personal information if the law specifies or otherwise indicates that information of a personal nature may be collected by the public body under the law for the "express" requirement in subsection 26 (a) to be met.

[95] Because there is no requirement in subsection 53 (b) that the law "expressly authorize[s]" the collection of an individual's personal health information, the threshold for determining when a law authorizes the collection of personal health information by a Custodian must be less. How much less must be considered in light of the purpose in subsection 1 (a) which is "to establish strong and effective mechanisms to protect the privacy of individuals with respect to their health information and to protect the confidentiality of that information." This purpose supports that the law cannot be so general as to vaguely imply that personal health information may be collected. To achieve the purpose in subsection 1 (a), the law, taken as a whole, must provide some clear implicit authority for a Custodian to collect personal health information.

[96] Under the HCIPA, the Director is charged with the responsibility of administering the Plan. The HCIPA authorizes her to collect information that she requires to administer the Plan. The Plan provides health care insurance to residents of Yukon. Physicians must submit billing claims under the Plan to the Director when they provide services insured by the Plan to residents.

[97] Section 8 of the HCIPR permits the Director to collect "any and all information" that she determines is required to substantiate the claims made by physicians under the Plan. While there are no purposes identified in the HCIPA, her obligations under the HCIPA, together with her duties as a public servant under the FAA, require her to administer the Plan in a fiscally responsible manner. To do so, she needs a certain amount of information to substantiate any billing claim made under the Plan.

[98] To substantiate a billing claim, she must collect at least some personal health information about a patient against whose insurance the claim is made. For this purpose, she must at least collect the patient's name, their Insurance Number, and the amount of the claim. She would also require additional personal health information, such as the service rendered, to pay the claim. She would need enough information both to satisfy herself that the claim is legitimate and that the claim made is registered for the correct patient.

[99] Based on the foregoing, I am satisfied that the HCIPA and HCIPR clearly imply that the Director has authority to collect an individual's personal health information for the purposes of paying physician billing claims for insured services rendered to the individual under the Plan.

[100] My finding, therefore, is that subsection 53 (b) authorizes the Director to collect the personal health information of Plan members for the purposes of remunerating Physician for claims submitted for services rendered to Plan members.

[101] My finding, in this regard, is consistent with the overarching purpose of HIPMA which, as I stated above, is to maximize the privacy and security of personal health information in the delivery of health care and the management of the health system, which necessarily includes facilitating the effective management of funding for the Plan.

[102] Given that I have found that the Custodian is authorized under subsection 53 (b) to collect the personal health information about Plan members for these purposes, I need not go on to consider whether subsection 53 (c) authorizes the collection.

Authority to indirectly collect and use personal health information

[103] The personal health information of Physician's patients when billing under the Plan is collected indirectly from Physician. As such, the Custodian must also have authority under section 54 for this indirect collection. The Custodian is relying on paragraph 54 (c)(i), together with paragraphs 56 (1)(b) and 56 (1)(o), as its authority for the indirect collection of the

personal health information. It is also relying on the same paragraphs in section 56 as its authority to use this information.

[104] These paragraphs state as follows.

> *54 A custodian may collect an individual's personal health information from a person other than the individual only if*
>
> *(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*[.]
>
> *56(1) A custodian may, without an individual's consent, use the individual's personal health information that is in its custody or control*
>
> *(b) subject to the requirements and restrictions, if any, that are prescribed, if an enactment of Yukon or Canada, or a treaty, arrangement or agreement entered into under such an enactment, permits or requires the use*
>
> *(o) for the purpose of*
>
> *(i) assisting in the prevention, detection or investigation of fraud in relation to health care, or*
>
> *(ii) preventing or reducing abuse in the use of health care*

56 (1)(b)

[105] There is no evidence before me that any of Physician's patients gave consent for the Custodian to use their personal health information. As such, I find that they did not.

[106] There are no prescribed requirements and restrictions on the use of personal health information contained in the Regulation in respect of paragraph 56 (1)(b).

[107] Yukon's *Interpretation Act*[28] defines an "enactment" as an Act or a regulation or any portion of an Act or a regulation". The HCIPA or HCIPR are, therefore, enactments.

---

[28] *Interpretation Act,* RSY 2002, c 125.

[108] In paragraph 46 of this Consideration Report, I determined the meaning of "required" in the context of HIPMA. For the Director to be required to use personal health information, the HCIPA or HCIPR must command or order her to use it. The HCIPA and HCIPR do not do so. Given this, I find the Custodian is not required to use the personal health information it collected or is otherwise in its custody or control to substantiate billing claims.

[109] As I indicated in paragraph 50 above, the HCIPA and HCIPR permit the Director to collect the personal health information that she needs to carry out her obligations, including for the purpose of substantiating billing claims submitted by Physician for services rendered to patients who are members of the Plan. It follows from this that she is also permitted by these laws to use this personal health information for this purpose.

[110] Given the foregoing, I find that the Custodian is authorized by paragraph 56 (1)(b) to use the personal health information it collects from Physician to process and pay the claims he submitted under the Plan for his patients, and by paragraph 54 (c)(i) together with paragraph 56 (1)(b) to also indirectly collect this information.

<u>56 (1)(0)</u>

There is no evidence before me that the Custodian is collecting personal health information from Physician for the purposes identified in this paragraph. As such, I find that the Custodian has not met its burden of proof in respect of its reliance on this paragraph. For this reason, it cannot rely on this paragraph to indirectly collect or use the personal health information from Physician.

<u>Sections 15 and 16</u>

[111] It is not enough that the Custodian has authority to collect and use personal health information under sections 53 and 54; it must also meet the requirements of sections 15 and 16 to have authority for the collection and use of the personal health information from Physician.

[112] These sections state as follows.

> *15 A person who is a custodian or the agent of a custodian must not collect, use or disclose personal health information if other information will serve the purpose of the collection, use or disclosure.*
>
> *16 The collection, use and disclosure of personal health information by a custodian or their agent must be limited to the minimum amount of personal health information*

that is reasonably necessary to achieve the purpose for which it is collected, used or disclosed.

Will information other than personal health information suffice?

[113] I have already determined that it is necessary for the Custodian to collect personal health information to process Physician billing claims. As such, I find that the Custodian has not collected personal health information contrary to the requirement in section 15.

Has the Custodian limited the collection of the personal health information to the minimum amount reasonably necessary?

[114] I am satisfied, based on the evidence provided by the Custodian through its written submissions and witness testimony, that it is reasonably necessary for it to collect the following personal health information from Physician for the purposes of remunerating Physician for services rendered:

a. E-billing System auto generated claim#; Physician's billing number; service date and time; number of services; patient name (first and last); name of family member or other third party when counselling involves these individuals; amount billed; fee code; and referring doctor billing number (where a referral is involved).

[115] I am satisfied that it would be necessary for the Custodian to collect an individual's Plan number to process Physician's claim made against their Plan number. Given that the Plan number is collected by the Custodian in relation to the provision of publicly-funded health care to the individual, it is not restricted by subsection 18 (1) from collecting it.

[116] An IHHS witnesses testified that IHHS needs to collect the ICD-9 code for each billing claim.[29] The privacy impact assessment (PIA) indicates that the ICD-9 code collected by IHHS to process billing claims is needed.[30] One witness testified that Physician included a description of the diagnoses for each billing claim in the comment field.[31] The document produced from Physician demonstrates this. The witness indicated that IHHS only needs the ICD-9 code and does not need additional information about diagnoses.[32] This same witnesses

[29]Director, IHHS, at p. 8, lines 19 and 20 of the transcript.

[30] PIA, p.74.

[31] Physician Claims Assessor, at p. 11 of the transcript, lines 6 to 17.

[32] Physician Claims Assessor, at p.11 of the transcript, lines 6 to 11.

noted, however, that on occasion, a physician may use the comment field to explain some anomaly associated with the services, such as where a surgery took longer than normal.[33]

[117] The meaning of ICD is "international classification disease for diagnosis.[34] Other than to define the term, the Custodian provided me with no evidence on why it collects the ICD-9 code. Given this, I had to resort to other sources for this answer.

[118] The Canadian Health Institute for Health Information states the following about the ICD-9 codes.

> *… a variety of medical classification standards were used in Canada for morbidity purposes. Two standards were in use at the national level for diagnosis classification: the International Statistical Classification of Diseases, Injuries, and Causes of Death, Ninth Revision (ICD-9) and the ICD-9-Clinical Modification (ICD-9-CM…*
>
> *The Ninth Revision of the International Classification of Diseases was approved by the 29th World Health Assembly in May 1976 to come into effect January 1, 1979. ICD-9 was adopted in Canada in 1979. ICD-9 is divided into two volumes: the Tabular List and the Alphabetic Index.*[35]

[119] The Government of British Columbia indicates the following on its website as to why it collects the ICD-9 codes for physician billing purposes.

> *Diagnostic Code Descriptions (ICD-9)*
>
> *All claims submitted by physicians to the Medical Services Plan (MSP) must include a diagnostic code. This information allows MSP to verify claims and generate statistics about causes of illness and death. The diagnostic codes used by MSP are based on the ninth revision of the International Classification of Diseases developed by the World Health Organization, commonly referred to as ICD9.*[36]

[120] A research article authored by individuals associated with the University of Calgary Department of Community Health Sciences and others from other jurisdictions examined the

---

[33] Physician Claims Assessor, at p.11 of the transcript, lines 13 to 17.

[34] Director, IHHS, at p. 8, lines 19 and 20 of the transcript.

[35] Canadian Institute of Health Information website at: https://www.cihi.ca/en/submit-data-and-view-standards/icd-9ccp-and-icd-9-cm.

[36] Government of British Columbia website at: https://www2.gov.bc.ca/gov/content/health/practitioner-professional-resources/msp/physicians/diagnostic-code-descriptions-icd-9.

use of ICD-9 codes across Canada in hospital. The article indicates that all provinces and territories use this coding system to track population health data.[37]

[121] Each ICD-9 code has a description of the diagnoses for each patient to whom a physician provides services. On the Custodian's website is the ability to search ICD-9 codes by diagnoses. For each of the billing claims submitted by Physician, I entered the diagnoses and found the corresponding ICD-9 code. Given this, I am satisfied that the Custodian collected no more personal health information than it would have had Physician entered the ICD-9 code instead of the diagnoses.

[122] Taken together, I am satisfied that the Custodian has authority to collect the ICD-9 codes and does so for the purpose of verifying billing claims and likely for population health purposes.

[123] As for the personal health information in the clinic record, two witnesses testified that the Custodian endeavoured to collect more personal health information from Physician than was necessary to process his fee code 610 billing claim.[38] Based on the evidence of these two witnesses, I am not satisfied the Custodian collected the minimum amount of personal health information from Physician to process his fee code 610 billing claim.

[124] Both witnesses confirmed that IHHS did not need all the personal health information contained in the clinic record it was endeavouring to collect from Physician to process his code 610 billing claim.[39]

[125] One witness confirmed that they do not need some of the more sensitive personal health information that may have been contained in this record in order to process Physician's code 610 billing claim.[40] The process adopted by IHHS on January 1, 2017, provides an example of the more sensitive personal health information that physicians should now redact before providing a copy of clinic record to IHHS. Both IHHS witnesses verified that IHHS does not need this sensitive personal health information.[41] One witness testified that the clinic record requested from Physician was a copy of the non-redacted clinic record

---

[37] See https://prism.ucalgary.ca/bitstream/handle/1880/49167/Walker_HSR_2012.pdf?sequence=1.

[38] Director, IHHS, at pp. 46 to 47 of the transcript; and Manager, Registration, Medical Travel and Hospital and Physician Claims, at pp. 31 to 33 of the transcript.

[39] *Ibid.*

[40] Director, IHHS, at pp. 46 to 47 of the transcript.

[41] Director, IHHS, at pp. 46 to 47 of the transcript; and Manager, Registration, Medical Travel and Hospital and Physician Claims, at pp. 31 to 33 of the transcript.

associated with his code 610 billing claim. The reason for this request was that the new process had not yet come into effect.[42]

[126] Based on the foregoing, I find that the Custodian collected the minimum amount of personal health information that was reasonably necessary to process Physician's billing claims submitted to it through its E-billing System. I also find, however, that the Custodian's collection of the non-redacted clinic record from Physician amounted to a collection of personal health information that was more than the minimum amount reasonably necessary to process Physician's fee code 610 billing claim.

Has the Custodian limited the use of the personal health information to the minimum amount reasonably necessary?

[127] I have reviewed the records submitted by Physician whose claims were verified by IHHS witnesses as processed. It is clear from these records that IHHS used all the personal health information it collected from Physician via its E-billing System to process these claims and that it was reasonably necessary that it do so. Given this, I find the Custodian used the minimum of personal health information amount reasonably necessary to process Physician's billing claims.

Finding – Issue 1

[128] My findings on Issue 1 are as follows.

a. The Custodian has authority under subsection 53 (b) and paragraphs 54 (c)(i) and 56 (1)(b) for the collection, indirect collection, and use of personal health information from Physician for the purpose of remunerating Physician for services rendered.

b. The Custodian met the requirements of section 16 for when it collected the personal health information from Physician via its E-billing System to process the billing claims submitted by Physician for the purpose of remunerating Physician for services rendered and used it for this same purpose.

c. The Custodian did not meet the requirements of section 16 for its collection of a copy of the non-redacted clinic record from Physician to process his code 610

[42] Manager, Registration, Medical Travel and Hospital and Physician Claims, at pp. 31 to 33 of the transcript.

billing claim for the reason that it did not limit the collection of personal health information to that which was reasonably necessary for the purpose of collection.

[129] Although I found that the Custodian's collection of personal health information in the clinic record contravened section 16, I acknowledge that following the Complaint Period[43] the Custodian modified its process of collecting information from physicians who are required to submit additional information, such as a copy of a clinic record, beyond that collected through the E-billing System to substantiate billing claims. As part of this process, the Custodian has defined a process whereby physicians are responsible for redacting sensitive personal health information that is not necessary for IHHS to collect from records they submit to IHHS to substantiate a billing claim. The Manual provides physicians with guidance on the kind of personal health information to redact and instructs IHHS employees to inform physicians about the need to redact this information prior to sending these records to them. The Manual is silent, however, on the obligations of IHHS employees who receive a letter that is not redacted. Without clear instruction about how to address this occurrence leaves the potential for the Custodian to be offside section 16.

[130] I note here that whether the Custodian is collecting more information than is necessary through its new process is not before me. Therefore, I did not consider this issue. To ensure the new process is compliant with section 16, the Custodian should examine its new process carefully to ensure it is meeting its collection and use obligations under HIPMA in regards to the collection and use of this personal health information in clinic records from physicians.

[131] Given the amount of public attention that occurred in respect of its practice of collecting clinic records or other similar kinds of records from physicians that may contain sensitive personal health information, it may wish, as part of examining this practice, to consult with the Yukon Medical Council (YMC) to ensure that physicians' views, as well as their respective corresponding legal obligations under HIPMA, are taken into account. Involvement of the YMC is also important, in my view, to ensure that any agreed upon process is communicated to physicians so that it can effectively be put into practice. In accordance with my duty to monitor compliance of HIPMA and to achieve the goal of maximizing the privacy and security of Yukoners' personal health information, I would be pleased to participate in this examination if invited to do so.

[43] The Complaint Period is between August 31, 2016 and November 28, 2016.

ISSUE 2: Do the measures in place to protect the security of the personal health information collected by the **[Custodian]** ***from Physician that is in the*** **[Custodian's]** ***custody and control meet the requirements of HIPMA?***

[132] The evidence provided by the Custodian about its security measures is as follows.

[133] The Custodian included with its submissions a schedule containing the security measures it has or will have in place (Schedule) in regards to the personal health information in its custody or control that it collected from Physician.

[134] The Schedule identifies a number of the security measures referenced above. It identifies physical measures, such as locked doors and filing cabinets, a file room and offices that are locked, a process for managing faxes received electronically, the handling of paper physician claims records for processing claims and review by the Yukon Medical Advisor, use of secure file transfer for transmission of personal health information, management of reciprocal claims communication, access controls for the E-billing System, individual credential use, use of PIAs, location of servers and their security, termination of access privileges when employees leave, use of screen-lock when computer unattended, destruction of record procedures, processes designed for secure transfer of records to archives, use of mandatory HIPMA compliance training, and visitor tracking mechanisms. The Custodian also identified in the Schedule that it plans to increase the security of the E-billing System and that it is reviewing physical security for improvement.

[135] It also submitted the following in regards to these and other information security measures.

> *The Director has implemented, or is in the process of implementing, various policies at IHHS including:*
>
> a. *IHHS Physician Claim Review/Audit Policy Manual*
> b. *a removable media and laptops policy;*
> c. *a clean desk policy; and*
> d. *a general office workplace security policy.*[44]
>
> *The Director continues to work on other measures to increase and improve the security of PHI at IHHS, as set out in* [the Schedule].

[44] These were appended to the Director's Statutory Declaration.

It is respectfully submitted that IHHS is meeting the requirements of s. 19 of the HIPMA and of s. 14 of [the Regulation].

There are measures in place "that protect the confidentiality, privacy, integrity and security of personal health information and that prevent its unauthorized modification" – see general office workplace security policy.

Controls are in place "that limit the individuals who may use personal health information to those specifically authorized by the custodian to do so" – see general office workplace security policy, removable media and laptop policy and clean desk policy.

Controls are in place "to ensure the 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;" – see bullets in [the Schedule] *re. software access limitations, control and printing of faxes, storage of paper records, access to physician records for adjudicative purposes and the three policies.*

Reasonable steps have been taken to prevent a security breach – see bullets in [the Schedule] *re. software access limitations, control and printing of faxes, storage of paper records, access to physician records for adjudicative purposes and the three policies.*

IHHS does "provide for the secure storage, disposal and destruction of records to minimize the risk of unauthorized access to, or disclosure of, personal health information;" – see bullets in [the Schedule] *relating to records management.*

IHHS does generally meet the prescribed requirements for retention of PHI, for receiving and responding to complaints re its practices, and as set out in s. 14 of [the Regulation].

The Director does not claim perfection. The Director acknowledges that security practices can always be improved and is steadily working with her staff to that end.

[136] A copy of the Manual was attached to the Affidavit of the Director along with the following policies.

a. Removable Media and Laptops policy. The date of issue is "January 9, 2017." As indicated by its title, this policy establishes rules that IHHS employees must follow in regards to removable media and laptops.

b. Clean Desk Policy. The date of issue is "January 9, 2017." Also as indicated by its title, this policy establishes rules that IHHS employees must follow to protect personal health information in their work area and in filing cabinets and key management.

c. General Office Workplace Security Policy. The date of issue is "January 9, 2017." This policy contains some specific rules designed to "protect the privacy and security of PHI or other sensitive information, to reduce the risk of security breaches in the workplace and increase employee's awareness about protection PHI and other sensitive information."

[137] In the Complainant's submissions, his only comments in respect of the Custodian's security practices were his concern with the lack of documented procedures and concerns in respect of its recycling practices.[45]

[138] In my Notice to Produce Records to the Custodian dated October 26, 2017, I asked the Custodian, *inter alia*, to produce the following records.

> 3. [P]*olicies, procedures, codes or other documents used by IHHS during the Complaint Period that support its authority to collect or use the PHI provided by or requested from the [Physician].*
>
> 4. *Any written policies, procedures or other documents that relate to IHHS's obligations under Division 3 of Part 3 in HIPMA and sections 14 and 16 of the* [Regulation]…
>
> 5. *Privacy impact assessments and security threat risk assessments conducted in relation to the billing claims procedures and information system used to process the PHI received or requested from the* [Physician] *during the Complaint Period.*

[45] Complainant submissions dated March 9, 2018 following the oral hearing.

[139] The response to this request by the Custodian is as follows.

a. The response to request #3 was "[t]here were no written policies in place during the [C]omplaint [P]eriod."

b. The relevant information to response #4 was (in general) that:

   i. the Manual was not implemented until after the Complaint Period;

   ii. role-based access was in effect prior to or during the Complaint Period;

   iii. IHHS employees received privacy training prior to or during the Complaint Period;

   iv. IHHS employees did not sign confidentiality pledges until after the Complaint Period; and

   v. auditing was not implemented until after the Complaint Period.[46]

[140] The Custodian also submitted a PIA that it conducted on the E-billing System dated April 30, 2017. This PIA contains a detailed analysis of the system, identifies a number of privacy and security policies and procedures HSS has in place, and identifies a number of risks to be addressed.

[141] As previously identified, the only personal health information the Custodian collected from Physician is the information submitted by Physician in his billing claims via his EMR to the E-billing System operated by HSS. Given this, my focus for this issue will solely be on the security measures that the Custodian had in place in respect of the E-billing System during the Complaint Period, which is August 31, 2016 to November 28, 2016.

[142] The minimum requirements that it must meet for the personal health information processed by the E-billing System are those set out in section 19 of HIPMA and section 14 of the Regulation. These provisions state as follows.

---

[46] Letter from S. Samis, November 10, 2017. Some relevant information was excluded from this Consideration Report, given that inclusion in a public document could create risks to the security of personal health information.

Section 19 (HIPMA) and Section 14 (Regulation)

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

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.

[143] The requirements in section 19 of HIPMA, together with section 14 of the Regulation, are not discretionary; they are mandatory. This means that the Custodian must, at minimum, meet all these requirements to be compliant with section 19.

[144] While the Custodian had some privacy policies and security procedures in place, as well as some physical and security safeguards prior to or during the Complaint Period as evidenced by the PIA and the submissions, it is clear that they had not, during this time period, met all the requirements required by section 19 in respect of the personal health information in the E-billing System. As such, there is no need for me to analyze each requirement to make the finding that as of November 28, 2016,[47] the Custodian had not met the requirements of section 19 of HIPMA, and my finding is as such.

[145] I appreciate that HIPMA has a lot of information security requirements to be met and that HSS has met some of them and is working towards meeting them all. However, it has work to do, in my view, to achieve this objective. The fact that the Custodian conducted a PIA on the E-billing System and submitted it to me for review and comment demonstrates its commitment to this work and I commend the Custodian for taking this important step.

[146] Having examined the PIA for this issue, I was able to determine that it identifies some risks of non-compliance with the information security requirements in HIPMA and that it contains a plan to address those risks. There are, however, in my view, a number of risks that have not been identified in the PIA. Consequently, there appears to be no plan to address them. As such, the Custodian will need to work with the IPC to properly identify the risks of non-compliance in the PIA for personal health information processed by the E-billing System and to ensure that a plan to mitigate those risks is included in the PIA.

[47] The end date of the Complaint Period.

Finding - Issue 2

[147] My finding on Issue 2 is that during the Complaint Period,[48] the measures that the Custodian had in place to protect the security of personal health information collected by the Custodian from Physician, and in the Custodian's custody and control, do not meet the requirements of HIPMA, specifically those in section 19.

IX FINDINGS

[148] As previously indicated, my findings on the issues in this Consideration are as follows.

[149] On Issue 1, I find as follows:

a. The Custodian has authority under subsection 53 (b) and paragraphs 54 (c)(i) and 56 (1)(b) for the collection, indirect collection and use of personal health information from Physician for the purpose of remunerating Physician for services rendered.

b. The Custodian did meet the requirements of section 16 for the collection and use of the personal health information it collected from Physician via its E-billing System to process the billing claims submitted by Physician for the purpose of remunerating Physician for services rendered.

c. The Custodian did not meet the requirements of section 16 for the collection of personal health information in the clinic record when it endeavoured to collect this record from Physician to process his code 610 billing claim for the reason that it did not limit the collection to that which was reasonably necessary.

[150] On Issue 2, I find as follows:

a. As of November 28, 2016,[49] the measures that the Custodian had in place to protect the security of personal health information collected by the Custodian from Physician, and in the Custodian's custody and control, do not meet the requirements of HIPMA, specifically those in section 19.

---

[48] The end date of the Complaint Period.

[49] *Ibid.*

X RECOMMENDATIONS

[151] My recommendations in regards to the issues are as follows.

[152] On Issue 1, my recommendation is as follows.

a. I recommend that the Custodian review its practice of collecting a copy of the clinic record from Physician to ensure that this collection and use of personal health information from Physician meets the requirement in section 16 of HIPMA. The Custodian must provide me with the steps it takes to give effect to this recommendation within six months of its acceptance.

[153] On Issue 2, my recommendation is as follows.

a. I recommend that the Custodian work with the OIPC in good faith on ensuring that the PIA it submitted for the E-billing System properly and adequately identifies the risks of non-compliance with the information security requirements in HIPMA and that its plan to mitigate those risks, within reasonable timeframes, is incorporated into the PIA. This work is to begin within 90 days of the date the Custodian accepts this recommendation.

X PUBLIC BODY’S DECISION AFTER REVIEW

[154] Subsection 112 (1) requires that within 30 days after receiving this Consideration Report, the Custodian must:

(a) decide whether to follow any or all of the recommendations of the commissioner; and

(b) give written notice of their decision to the commissioner.

[155] Subsection 112 (2) states that “[i]f [the Custodian] does not give written notice within the time required by subsection (1), [the Custodian] is deemed to have decided not to follow any of the recommendations of the commissioner.”

XI APPLICANT'S RIGHT OF APPEAL

[156] The Complainant's right of appeal is set out in section 114. It states as follows.

> *114 Where a report includes a recommendation, and* [the Custodian] *decides, or is deemed to have decided, not to follow the recommendation, or having given notice of its decision to follow the recommendation has not done so within a reasonable time, the complainant may, within six months after the issuance of the report, initiate an appeal in the court.*

____

Diane McLeod-McKay, B.A., J.D.
Yukon Information and Privacy Commissioner

Distribution List:

- Custodian
- Complainant

Postscript

Production of Records for Consideration

During the course of this Consideration, I experienced a number of challenges in obtaining sufficient evidence from the Custodian to decide the issues.

In response to the Notice of Consideration that identified the issues for consideration, I received submissions from the Custodian. Included with these submissions were legal arguments about the application of HIPMA together with information about the Custodian's security measures in place to protect personal health information in its custody or control.

As part of its submission, the Custodian did not provide any evidence about whether the Custodian collected or tried to collect personal health information from Physician. Nor did it provide any records evidencing or refuting the collection. Without this evidence, it would have been impossible for me to decide the issues.

In response to my Notice to Produce Records issued to Physician, I received records that indicated Physician had submitted 200 billing claims to the Custodian between August 31, 2016 and November 28, 2016 (the Complaint Period). The Custodian's response to its Notice to Produce Records was that it had no records relevant to the Consideration.

Despite this assertion, it was clear to me that the Custodian must have records of or related to these billing claims that would contain personal health information and would, therefore, be relevant to the Consideration. Given this, I determined it was necessary to conduct an oral hearing so that I could obtain evidence directly from Physician and the Custodian about these billing claims.

During the oral hearing, I learned that Physician did submit the billing claims to IHHS that were in the records he provided[50] and that the personal health information associated with these billing claims is contained within the E-billing System and accessible in numerous formats throughout the Consideration.[51]

My ability to obtain the evidence I need to consider complaints under HIPMA is dependent on the cooperation of parties. It is apparent that the Custodian had records relevant to the Consideration but failed to produce them. My realization of this fact during the course of considering the issues required that I conduct an oral hearing, which took a significant amount of time and cost to complete.

One witness acknowledged during the oral hearing that the Custodian failed to preserve records; namely, the suspended claim report that was relevant to this Consideration, despite their knowing it was underway and that it had moved to adjudication. This, in my view, is serious. Nevertheless, I believe that this occurred unintentionally and I appreciate the honesty of this witness in acknowledging this fact.

What occurred in this case demonstrates that there is a need for Custodians to ensure that once they are involved in the consideration process, whether informal or formal, they must actively identify relevant evidence and preserve it. They must also produce this evidence to the IPC to assist her and her investigators in concluding a consideration in a timely manner. Failure to take these actions leads to considerable delay in resolving considerations,

---

[50] Manager, Registration, Medical Travel and Hospital and Physician Claims, at p. 59 of the transcript.

[51] Manager, Registration, Medical Travel and Hospital and Physician Claims, at pp. 61 to 65 of the transcript; and Manager of Health Informatics and Information Technology, at p. 29 of the transcript.

unnecessary expense of public funds to conclude a consideration, and has a negative impact on complainants who have no control over the process and are left to endure lengthy delays.

As Custodians move more and more into processing personal health information electronically, any preservation of evidence will necessarily involve searching electronic information systems for these records and storing this information in such a manner as to ensure its availability and integrity through the proceeding.