

ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

ORDER H2022-04

March 31, 2022

ALBERTA HEALTH SERVICES

Case File Number 023858

Office URL: www.oipc.ab.ca

Summary: An individual made a complaint under the *Health Information Act* (the Act) that her health information and that of her two minor children (Child A and Child B) in the Alberta Electronic Health Record (the EHR, commonly referred to as Netcare) had been accessed numerous times without authority by a number of employees of Alberta Health Services (the Custodian).

The individual further complained that Child A's health information in the Clinibase electronic medical record system (Clinibase) and the Sunrise Clinical Manager electronic medical record system (the SCM) had been accessed without authority by employees of the Custodian.

The complaints about the accesses to the individual's own health information, and Child B's health information were addressed in separate inquiries. This inquiry deals only with the complaints the individual made about accesses to Child A's health information in the EHR/Netcare, Clinibase and the SCM by the employees of the Custodian. Child A is the Complainant in this inquiry.

The Adjudicator determined that with the exception of one access made by one employee of the Custodian in 2013 to the Complainant's health information in Clinibase, and three accesses made in 2013 to the Complainant's health information in Netcare PD by another employee of the Custodian, the accesses to the Complainant's health information by the Custodian's employees were in compliance with Part 4 of the Act.

The Adjudicator determined that one access made by one employee of the Custodian to the Complainant's health information in Clinibase in 2013, and three accesses made by another employee of the Custodian to the Complainant's health information in Netcare PD in 2013, were in contravention of Part 4 of the Act.

The Adjudicator determined that the Custodian had met its duty to take reasonable steps to maintain administrative, technical and physical safeguards to protect the confidentiality of health information under section 60 of the Act.

Statutes Cited: AB: *Health Information Act*, R.S.A. 2000, c. H-5, ss. 1, 25, 27, 28, 56.1, 56.5, 60, 62, 80 and 104.

Regulations Cited: AB: *Health Information Regulation*, AR 70/2001 and *Alberta Electronic Health Regulation*, AR 118/2010.

Authorities Cited: AB: Investigation Report H2018-IR-01 and Orders H2020-04, F2020-12, H2021-01, H2021-06 and H2022-01.

Cases Cited: *Gowrishankar v JK*, 2018 ABQB 70; *JK v Gowrishankar*, 2019 ABCA 316.

I. BACKGROUND

[para 1] On April 12, 2016, this Office received a complaint from an individual (the Mother) that her health information was accessed in the Alberta Electronic Health Record (the EHR, commonly referred to as Netcare) without authority under the *Health Information Act*, R.S.A. 2000, c. H-5 (the HIA or the Act) numerous times, by various individuals employed by Alberta Health Services (the Custodian).¹

[para 2] The Mother also complained on behalf of her two minor children, (whom I will refer to as Child A and Child B), that their health information was accessed in the EHR/Netcare without authority under the Act numerous times, by various individuals employed by the Custodian.²

[para 3] The Mother also complained that Child A's, health information in the Clinibase electronic medical record system (Clinibase) was accessed without authority by an individual employed by the Custodian.

¹ Complainant's Mother's Request for Review/Complaint received April 12, 2016.

² Section 104(1)(c) of the Act permits the guardian of an individual who is under 18, and who does not meet the criterion in clause (b), to exercise any right or power conferred on an individual by the Act.

[para 4] In addition, the Mother complained that Child A's health information in the Sunrise Clinical Manager electronic medical record system (the SCM) was accessed without authority by individuals employed by the Custodian.

[para 5] The Commissioner appointed a Senior Information and Privacy Manager to investigate and attempt to settle the matter. Subsequently, the Mother requested an inquiry into the accesses to her health information and the health information of her two children, in the EHR/Netcare, and the accesses to Child A's health information in Clinibase and the SCM.³

[para 6] The Commissioner agreed to conduct an inquiry and delegated her authority to conduct the inquiry to me.

[para 7] By way of letter dated November 12, 2021, I asked Child A's Mother to inform me whether Child A had now turned 18, as the information before me indicated that this may have been a possibility. If so, I requested that Child A confirm to me that she wished this inquiry to continue, and if so, to complete this Office's Change of Contact and/or Address for Service form (the Form). The Form contains a box to check if an individual is authorizing someone to act on their behalf.

[para 8] On November 22, 2021, Child A's Mother e-mailed the Form, signed by Child A. Child A indicated that she authorized her Mother to act on her behalf for the purposes of this complaint.

[para 9] Neither Child A's Mother nor Child A complied with my requests exactly. Child A's Mother did not inform me if Child A had in fact, turned 18. Nor did Child A specifically state that she wished this inquiry to continue.

[para 10] However, since Child A had completed the Form, I advised the parties that I would interpret the Form that Child A signed as her indication that she wished the inquiry to continue, and that she was either 18, in which case section 104(1)(a) of the HIA applied, or, alternatively, that she was under 18 and understood the nature of the right or power and the consequences of exercising the right or power, in which case section 104(1)(b) of the HIA applied.⁴

[para 11] The inquiry was then divided into three separate inquiries: one for the Mother, one for Child A and one for Child B. This inquiry deals solely with the complaints the Mother made regarding accesses to Child A's health information in the EHR/Netcare, Clinibase and the SCM by the employees of the Custodian.

[para 12] Child A is the sole Complainant in this inquiry. All submissions in this inquiry have been made on her behalf by her Mother.

³ Complainant's Mother's Request for Inquiry received May 23, 2017.

⁴ Letter to Parties dated December 3, 2021. As I do not have confirmation that Child A has now turned 18, she will be referred to in this inquiry as Child A or the Complainant.

II. ISSUES

[para 13] The issues for this inquiry are as follows:

- 1. Did the Custodian or its Affiliates use the Complainant's health information in contravention of Part 4 of the HIA?**
- 2. Did the Custodian fail to safeguard the Complainant's health information in contravention of section 60 of the HIA?**

Scope of Inquiry

[para 14] The Complainant's Mother provided a copy of the Complainant's Netcare audit log, showing the accesses to the Complainant's health information in the EHR/Netcare for the period January 1, 2010 to March 3, 2016, with her Request for Review/Complaint Form. In addition, the Complainant's Mother provided a copy of the Complainant's Clinibase Audit Report for the period January 1, 2011 to January 26, 2016. The Complainant's Mother also provided a copy of the Complainant's SCM Audit Log dated February 10, 2016.

[para 15] The Complainant's Mother attached a page titled "Statement of Claim" to her Request for Review/Complaint Form. The Complainant's Mother attached a handwritten list to the page titled "Statement of Claim" in which she identified the accesses to the Complainant's health information in the EHR/Netcare, Clinibase and the SCM, recorded in the Complainant's EHR/Netcare, Clinibase and the SCM audit logs, which she alleged were made in contravention of the Act by employees of the Custodian.

[para 16] The Complainant's Mother also made multiple additional allegations in her submissions about individuals accessing, using and/or disclosing the Complainant's health information, located in the EHR/Netcare system or in paper files. The Complainant's Mother provided no evidence to support these allegations and they do not form part of this inquiry.

[para 17] This scope of this inquiry is limited to reviewing only those accesses by the Custodian or its Affiliates to the Complainant's health information in the EHR/Netcare, Clinibase and the SCM, which the Complainant's Mother identified in item numbers 1 – 12 and 39 of her handwritten list, for which there was supporting evidence in the Complainant's Netcare audit log, the Clinibase audit log and the SCM audit log, and determining whether those specific accesses were made in contravention of, or in compliance with the Act.

III. DISCUSSION OF ISSUES

- 1. Did the Custodian or its Affiliates use the Complainant's health in contravention of Part 4 of the HIA?**

[para 18] Section 25 of the Act prohibits a custodian from using health information unless a provision of the Act authorizes doing so. It states:

25 No custodian shall use health information except in accordance with this Act.

[para 19] The Act defines “custodian” in section 1(1)(f)(iv) to include “a regional health authority established under the *Regional Health Authorities Act*”.

[para 20] Alberta Health Services is a custodian under the Act.⁵

[para 21] “Health information” is defined in section 1(1)(k) of the Act as follows:

1(1) In this Act,

(k) “health information” means one or both of the following:

- (i) diagnostic, treatment and care information;*
- (ii) registration information;*

[para 22] “Diagnostic, treatment and care information” is defined in section 1(1)(i) of the Act as follows:

1(1) In this Act,

(i) “diagnostic, treatment and care information” means information about any of the following:

- (i) the physical and mental health of an individual;*
- (ii) a health service provided to an individual, including the following information respecting a health services provider who provides a health service to that individual;*
 - (A) name;*
 - (B) business title;*
 - (C) business mailing address and business electronic address;*
 - (D) business telephone number and business facsimile number;*
 - (E) type of health services provider;*

⁵ Custodian’s submission dated May 14, 2021 at para. 18. See too, Order H2020-04 at para. 14.

- (F) *license number or any other number assigned to the health services provider by a health professional body to identify that health services provider;*
 - (G) *profession;*
 - (H) *job classification;*
 - (I) *employer;*
 - (J) *municipality in which the health services provider's practice is located;*
 - (K) *provincial service provider identification number that is assigned to the health services provided by the Minister to identify the health services provider;*
 - (L) *any other information specified in the regulations;*
- (iii) *the donation by an individual of a body part or bodily substance, including information derived from the testing or examination of a body part or bodily substance;*
 - (iv) *a drug as defined in the Pharmacy and Drug Act provided to an individual;*
 - (v) *a health care aid, device, product, equipment or other item provided to an individual pursuant to a prescription or other authorization;*
 - (vi) *the amount of any benefit paid or payable under the Alberta Health Care Insurance Act or any other amount paid or payable in respect of a health service provided to an individual,*
- and includes any other information about an individual that is collected when a health service is provided to the individual, but does not include information that is not written, photographed, recorded or stored in some manner in a record;*

[para 23] “Registration information” is defined in section 1(1)(u) as follows:

1(1) In this Act,

- (u) *“registration information” means information relating to an individual that falls within the following general categories and is more specifically described in the regulations:*

- (i) *demographic information, including the individual's personal health number;*
- (ii) *location information;*
- (iii) *telecommunications information;*
- (iv) *residency information;*
- (v) *health and service eligibility information;*
- (vi) *billing information;*

but does not include information that is not written, photographed, recorded or stored in some manner in a record;

[para 24] Section 3 of the *Health Information Regulation*, AR 70/2001 states:

3 The following information, where applicable, relating to an individual is registration information for the purposes of section 1(1)(u) of the Act:

- (a) *demographic information, including the following:*
 - (i) *name, in any form;*
 - (ii) *signature;*
 - (iii) *photograph or electronic image of the individual's face for identification purposes;*
 - (iv) *personal health number or any other unique identification number that is used to identify the individual as eligible for, or a recipient of, a health service;*
 - (v) *gender;*
 - (vi) *date of birth;*
 - (vii) *birth information, including*
 - (A) *the birth facility; and*
 - (B) *birth order, in the case of a multiple birth*
 - (viii) *marital status;*
 - (ix) *date of death;*

- (x) *treaty status;*
 - (xi) *whether the individual is a registrant or a dependant of a registrant under the Health Insurance Premiums Act;*
- (b) *location, residency and telecommunications information, including the following:*
- (i) *home, business and mailing addresses, electronic address and telecommunications numbers;*
 - (ii) *health regions, as established under the Regional Health Authorities Act, in which the individual resides and previously resided;*
 - (iii) *citizenship or immigration status, including the date on which the individual's current immigration status expires if the individual is not a Canadian citizen or landed immigrant;*
 - (iv) *date of entry into Canada and into Alberta;*
 - (v) *province or country of birth or of last residence;*
 - (vi) *date on which the individual became or is expected to become a permanent resident of Canada;*
 - (vii) *in the event the individual is a registrant or dependant under the Health Insurance Premiums Act and the individual intends to be temporarily or permanently absent from Alberta,*
 - (A) *date of departure;*
 - (B) *destination and intended date of arrival at the destination;*
 - (C) *forwarding address;*
 - (D) *intended date of return, where the individual intends to be temporarily absent;*
 - (E) *purpose of absence;*
- (c) *health service eligibility information, including the following:*
- (i) *whether the individual is registered as a registrant or dependant under the Health Insurance Premiums Act;*

- (ii) *whether the individual is eligible to receive health services that are directly or indirectly paid for by the Government of Alberta, in full or in part;*
 - (iii) *whether the individual has elected to opt out of the Alberta Health Care Insurance Plan and the Hospitalization Benefits Plan;*
 - (iv) *whether the individual is exempt from the requirement to register under the Health Insurance Premiums Act;*
 - (v) *whether the individual is eligible to receive a reduction or waiver of premiums or charges payable in respect of health services and the level or amount or both, of that reduction or waiver;*
 - (vi) *information about any program of a custodian that is related to the information described in subclauses (i) to (vi), including the effective and termination dates of the program and, if applicable, the program name;*
- (d) *billing information, including the following:*
- (i) *information about amounts owed by the individual to the custodian;*
 - (ii) *method of payment;*
 - (iii) *the individual's account number;*
 - (iv) *if another person is liable for or will be billed for the amount owed by the individual, that person's name and account number.*

[para 25] Section 1(1)(w) of the Act defines “use” as follows:

1(1) In this Act,

- (w) *“use” means to apply health information for a purpose and includes reproducing the information, but does not include disclosing the information.*

[para 26] The circumstances in which a custodian may use health information are set out in section 27 of the Act. Section 27(1) states:

27(1) A custodian may use individual identifying health information in its custody or under its control for the following purposes:

- (a) *providing health services;*
- (b) *determining or verifying the eligibility of an individual to receive a health service;*

- (c) *conducting investigations, discipline proceedings, practice reviews or inspections relating to the members of a health profession or health discipline;*
- (d) *conducting research or performing data matching or other services to facilitate another person's research*
- ...
- (e) *providing for health services provider education;*
- (f) *carrying out any purpose authorized by an enactment of Alberta or Canada;*
- (g) *for internal management purposes, including planning, resource allocation, policy development, quality improvement, monitoring, audit, evaluation, reporting, obtaining or processing payment for health services and human resource management.*

[para 27] The definition for a “health service” is set out in section 1(1)(m) of the Act as follows:

1(1) In this Act,

- (m) *“health service” means a service that is provided to an individual for any of the following purposes:*
 - (i) *protecting, promoting or maintaining physical and mental health;*
 - (ii) *preventing illness;*
 - (iii) *diagnosing and treating illness;*
 - (iv) *rehabilitation;*
 - (v) *caring for the health needs of the ill, disabled, injured or dying,*
but does not include a service excluded by the regulations.

[para 28] Section 28 of the Act regulates the use of health information by an affiliate. It states:

28 An affiliate of a custodian must not use health information in any manner that is not in accordance with the affiliate's duties to the custodian.

[para 29] “Affiliate” is defined in section 1(1)(a) of the Act as follows:

1(1) In this Act,

- (a) “affiliate”, in relation to a custodian, means
- (i) an individual who is employed by the custodian,
 - (ii) a person who performs a service for the custodian as an appointee, volunteer or student under contract or agency relationship with the custodian,
 - (iii) a health services provider who is exercising the right to admit and treat patients at a hospital as defined in the *Hospitals Act*,
 - (iv) any information manager as defined in section 66(1), and
 - (v) a person who is designated under the regulations to be an affiliate, but does not include
 - (vi) an agent as defined in the *Health Insurance Premiums Act*, or
 - (vii) a health information repository other than a health information repository that is designated in the regulations as an affiliate;

[para 30] As noted by the adjudicator in Order H2020-04 at paragraph 6:

[para 6] The legislative scheme governing health information and the access of the EHR changed in 2010. On September 1, 2010, Part 5.1 of the HIA came into force. The provisions of Part 5.1 contain authority for the creation of the EHR and establish the authority for custodians to use electronic health information stored on this system.

[para 31] In Order F2020-12, the adjudicator described the Alberta EHR at paragraph 15 as follows:

[para 15] “Netcare” (referred to in the HIA as the “Alberta EHR”) is an integrated electronic health information system, within the terms of section 56.1 of the *Health Information Act* (HIA). AHS’s use of Netcare is governed by Part 5.1 of the HIA. The information housed in Netcare is “health information” within the terms of section 1 of the HIA ...

[para 32] As stated in previous Orders of this Office, accessing health information in the EHR/Netcare is considered to be a “use” of health information under the Act.⁶

[para 33] Section 56.5 of the Act sets out the circumstances in which authorized custodians may use health information in the EHR. It states:

56.5(1) Subject to the regulations,

⁶ See, for example, Orders H2020-04 at paras. 7 and 71, H2021-01 at paras. 17 and 19, and H2021-06 at para. 8

- (a) *an authorized custodian referred to in section 56.1(b)(i) may use prescribed health information that is accessible via the Alberta EHR, for any purpose that is authorized by section 27;*
- (b) *an authorized custodian referred to in section 56.1(b)(ii) may use prescribed health information that is accessible via the Alberta EHR, and that is not otherwise in the custody or under the control of that authorized custodian, only for a purpose that is authorized by*
 - (i) *section 27(1)(a), (b) or (f), or*
 - (ii) *section 27(1)(g), but only to the extent necessary for obtaining or processing payment for health services.*
- (2) *For greater certainty, the use pursuant to subsection (1) of prescribed health information that is accessible via the Alberta EHR does not constitute collection of that information under this Act.*
- (3) *For greater certainty, the use pursuant to subsection (1) of prescribed health information that is accessible via the Alberta EHR does not constitute a disclosure of that information by*
 - (a) *the regulated health professional or authorized custodian who originally made that information accessible via the Alberta EHR pursuant to section 56.3,*
 - (b) *any other authorized custodian,*
 - (c) *the information manager of the Alberta EHR, or*
 - (d) *any other person.*

[para 34] Section 4 of the *Alberta Electronic Health Regulation*, AR 118/2010 sets out what “prescribed health information” in section 56.1(c) of the Act includes. It states:

4 For the purposes of section 56.1(c) of the Act, prescribed health information in respect of an individual includes:

- (a) *the demographic information that uniquely identifies the individual,*
- (b) *information that uniquely identifies health service providers who provide health services to the individual,*
- (c) *information about where health services are performed on and delivered to the individual,*
- (d) *information about key clinical events at the point of care in respect of the individual,*
- (e) *known allergies and intolerances of the individual,*

- (f) *immunizations of the individual,*
- (g) *prescription information in respect of the individual,*
- (h) *dispensing information relating to prescriptions in respect of the individual,*
- (i) *drug-to-drug interaction alerts in respect of the individual,*
- (j) *laboratory test results of the individual,*
- (k) *diagnostic imaging reports and tests of the individual,*
- (l) *diagnostic imaging digital images of the individual, and*
- (m) *other medical reports of the individual.*

[para 35] In this case, all of the accesses the Complainant’s Mother asserted in her handwritten list were made by the Custodian or its Affiliates to the Complainant’s health information in the EHR/Netcare in contravention of the Act, occurred after September 1, 2010.

[para 36] As noted above, Alberta Health Services is a custodian under section 1(1)(f)(iv) of the Act. Alberta Health Services is therefore an authorized custodian under section 56.1(b)(i) of the Act.⁷

[para 37] While section 56.5(1) only refers to the use of health information by “authorized custodians” and does not mention the use of health information by affiliates, section 62(2) states that any collection, use or disclosure of health information by an affiliate of a custodian is considered to be collection, use or disclosure by the custodian:⁸

62(2) Any collection, use or disclosure of health information by an affiliate of a custodian is considered to be a collection, use or disclosure by the custodian.

[para 38] Additionally, section 62(4) provides:

62(4) Each affiliate of a custodian must comply with

- (a) *this Act and the regulations, and*
- (b) *the policies and procedures established or adopted under section 63.*

⁷ See too Order H2021-06 at para. 11.

⁸ See Orders H2020-04 at paras. 16 – 19, H2021-01 at paras. 18 – 19, H2021-06 at paras. 15 – 16, and *Gowrishankar v. JK*, 2018 ABQB 70 at paras. 44 - 45 (upheld on appeal at *JK v. Gowrishankar*, 2019 ABCA 316).

[para 39] At paragraph 16 of Order H2021-06, the adjudicator made the following comments regarding the use of health information by affiliates:

[para 16] In *JK v. Gowrishankar*, 2019 ABCA, the Alberta Court of Appeal held that under section 62(2) affiliates have, subject to their duties with their custodian, the same authority as their related custodians to use health information. The Court stated at paras 25 to 28:

Turning next to affiliates of custodians. While there is no provision in the *HIA* that expressly authorizes an affiliate to collect, use, or disclose health information, this authorization is implicit in the Act. Section 62(2) provides that:

*62(2) Any collection, use or disclosure of health information **by an affiliate** of a custodian is considered to be a collection, use or disclosure by the custodian.*

(emphasis added)

This section contemplates that affiliates will be collecting, using, and disclosing health information. As a number of the defined custodians are entities, such as the department of the responsible Minister, it is the employees and contractors of those entities that collect, use, and disclose the information as prescribed by the *Act*. Because the *Act* permits a custodian to collect, use, and disclose information for specific purposes, its affiliates are also permitted to collect, use, and disclose the information for those same purposes. Indeed, this is the interpretation previously adopted by the OIPC: *Re Alberta Health and Wellness* (March 25, 2008), 2008 CanLII 88791 (AB OIPC), Order H2007-005 and Order P2007-013.

The nature of an affiliates relationship with the custodian imposes limitations on how an affiliate may collect, use and disclose health information. An affiliate may only collect, use or disclose health information in accordance with its duties to the custodian. This must be inferred from the provisions that prohibit affiliates from collecting, using or disclosing health information in a manner that is not in accordance with the affiliate's duties to the custodian: ss 24, 28, 43. Affiliates must also comply with any policies or procedures established by the custodian: s 63(4)(b).

In summary, the collection and use of health information by a custodian (including an authorized custodian) and its affiliates is authorized by the Act so long as i) it is for a purpose permitted by the Act; and ii) the information is essential to carry out the intended purpose. An affiliate is subject to further limitations based on the affiliate's duties to the custodian, and any policies or procedures put into place by the custodian. Custodians and affiliates are permitted to disclose health information with or without consent, depending on the circumstances.

[para 40] Accordingly, like the Custodian, an affiliate of the Custodian may use health information only for purposes set out in section 27 of the Act.

Accesses to the Complainant's health information in the EHR/Netcare, Clinibase and the SCM

[para 41] The Complainant's Mother questioned a number of accesses to the Complainant's health information that were shown in the Complainant's Netcare audit log, Clinibase audit log and SCM audit log.

[para 42] In item numbers 1 – 12 and 39 of the Complainant's Mother's handwritten list attached to her Request for Review/Complaint Form, the Complainant's Mother listed the accesses to the Complainant's health information in the EHR/Netcare, Clinibase and SCM which she believed were made without authority under the Act, and in some cases provided a reason why she believed the access was unauthorized, as follows:⁹

1. On Jan 21, 2011 my daughter's health records were viewed 5 times by "[Name]" on the AHS's SCM database.
2. Twice on Jan 31, 2011 "[same Name as in item number 1]" again accessed my daughter's health records on SCM.
3. Twice again on June 27, 2012 "[same Name as in item number 1]" accessed my daughters health records on SCM
4. On Feb 1, 2014 AHS's SCM database was accessed to view my daughter's health records by a "[Name]".
5. On April 23, 2013 AHS's clinibase was accessed by my co-worker "[Name]" to view my daughter's health records. There is absolutely no reason why my co-worker should be needing to access my daughters [sic] health records.
6. On Nov 4, 2011 AHS's Netcare database was accessed by "[Name]" to view my daughter's records
7. On Dec 12, 2011 AHS's Netcare database was accessed by "[Name]" to view my daughter's health records at [facility]
8. On Nov 8, 2012 AHS's Netcare database was accessed by "[Name]" at the [facility] to view my daughter's health records.
9. On April 5, 2013 AHS's Netcare database was accessed by "[Name]" at the [location/facility] to view my daughter's health records.
10. On Aug 22, 2013 AHS's Netcare database was accessed by "[same Name as in item number 9]" at the [location/facility] to view my daughter's health records.
11. On Sep 3, 2013 AHS's Netcare database was accessed by [same Name as in item number 9]" at the [location/facility] to view my daughter's health records
12. On Feb 1, 2014 AHS's Netcare database was accessed by "[Name]" at the [facility] to view my daughter's health records.
- ...
39. On Sep 25, 2014 AHS's Netcare database was accessed by "[Name]" to view my daughter's [Child A]'s health records.

⁹ Complainant's Mother's handwritten list attached to Complainant's Mother's Request for Review/Complaint Form received April 12, 2016.

[para 43] The Custodian advised that all of the accesses identified by the Complainant's Mother in item numbers 1 – 12 and 39 of her handwritten list, were made by individuals who were affiliates of the Custodian at the time they accessed the Complainant's health information. These accesses are, accordingly, within the scope of this inquiry.¹⁰

[para 44] The Custodian conducted an investigation and determined that with the exception of the one access by one employee to the Complainant's health information in Clinibase identified by the Complainant's Mother in item number 5 of her handwritten list, and the three accesses by another employee to the Complainant's health information in the EHR/Netcare identified by the Complainant's Mother in item numbers 9, 10 and 11 of her handwritten list, the remainder of the accesses the Complainant's Mother identified in her handwritten list were made by employees of the Custodian in compliance with either sections 27(1)(a) or (g) of the Act.¹¹

[para 45] As noted above, section 27(1)(a) permits a custodian to use health information in order to provide health services, and section 27(1)(g) permits a custodian to use health information for internal management purposes, including planning, resource allocation, policy development, quality improvement, monitoring, audit, evaluation, reporting, obtaining or processing payment for health services and human resource management.

[para 46] In its submission, the Custodian provided the following information about Clinibase, the SCM, and Netcare:¹²

...

4. SCM is the Electronic Medical Record (EMR) used by AHS in the Calgary zone. It provides patient-centric clinical information including: medical and nursing orders, electronic medication administration records, clinical documentation, and diagnostic imaging and lab results. The integrated view of the patient's chart also includes key demographic and visit information, as well as historical chart data. SCM consists of 3 modules:
 - SCM Acute Care which supports Inpatient locations
 - SCM Ambulatory Care which supports outpatient clinics
 - SCM Emergency Care (SEC) which supports Emergency departments
5. Clinibase is a system used to Admit, Discharge and Transfer patients. It is the source of information for patient identification and encounter management in all acute care sites and AHS community health centres in the Calgary and Rural zones. Clinibase generates the Regional Health Record Number which identifies each patient.

¹⁰ Custodian's submission dated May 14, 2021.

¹¹ *Ibid.*, at paras. 19, 22 – 23, and 75 – 78.

¹² *Ibid.*, at paras. 4 – 11.

6. Broad functionality includes initiating and tracking inpatient and outpatient services defined by an Encounter Number. Specific functionality includes; referrals, waitlists, pre-admissions/pre-registrations, bed management, transferring and discharging of patients and patient caseload management.
7. Information in Clinibase includes patient demographics, unit of clinic patient is admitted to, some basic health information gathered by the admitting clerk, family physician, attending and admitting, among other non-clinical information. Information in Clinibase flows to SCM to form the basic patient chart.
8. The Adjudicator has requested information about what each user viewed when accessing the Complainants' health information. The SCM did not have the ability to track this data until 2015, so unfortunately, there is no way to know precisely what was viewed in the SCM in the relevant timeframe. Information about what each user viewed in Clinibase and Netcare is provided below, in the description of each individual access.
9. Additionally, the Adjudicator has requested information about how SCM and Clinibase relate to Netcare. SCM and Clinibase are repositories of information operated by AHS. They are completely separate from Netcare and are not accessible through Netcare, which is a repository operated by Alberta Health. SCM and Clinibase must be accessed separately by authorized AHS users.
10. Access to patient information in Clinibase and SCM would not show up in a Netcare audit log. SCM and Clinibase are AHS applications and have their own audit logs that must be requested from AHS. In this case, the Complainants received audit logs from SCM, Clinibase and Netcare, and attached these to her Notice of Inquiry.¹³
11. AHS will slowly be transitioning off of both the Clinibase and SCM systems in favour of the Connect Care system. The transition is expected to take time, and both systems will likely be in place through 2023. Both systems remain active at this time.

[para 47] As I noted that in some of the accesses to the Complainant's health information in the SCM audit log indicated that the "User" was different from the "Attending physician", I asked the Custodian to provide an explanation for this. The Custodian provided the following information:¹⁴

The User is the individual who accessed the health information. The Attending Physician is the physician responsible for the care of the patient at the time of access. When an individual visits an AHS facility, there may be multiple people who require access to the patient's health information for a variety of reasons. This could include admission clerks, RNs and other affiliates involved in the care of the patient, or involved in health information management.

¹³ The Complainant's Mother's Request for Review/Complaint and attachments, which included the Complainant's audit logs, were enclosed as attachments to the Notice of Inquiry issued by this Office.

¹⁴ Custodian's submission dated May 14, 2021 at para. 12.

The Custodian also addressed this in its explanations in relation to the individual accesses below.

[para 48] The Custodian also provided the following information about the EHR/Netcare, Netcare PD, and the Netcare audit log:

13. Netcare is a repository that contains both demographic information and other health information about a patient. Netcare PD is an iteration of Netcare that only shows demographic information about a patient. Where 'Netcare PD' is noted in the audit log, only demographic information was accessible to the user.
14. One of the columns in the Netcare audit is titled 'Facility'. In general, this column denotes the primary facility to which the User is affiliated. However, it is not uncommon for AHS employees to work at multiple facilities which would not be reflected in this column. The 'Facility' column does not indicate the facility the user was at when they accessed the patient's health information.

Accesses Identified in Item Numbers 1 – 4, 6, 7, 8, 12 and 39

[para 49] The Custodian provided the following explanations for the accesses made by its employees to the Complainant's health information, identified in item numbers 1 – 4, 6, 7, 8, 12 and 39 of the Complainant's Mother's handwritten list, which the Custodian determined were authorized under the Act. For each of these item numbers, the Custodian referenced what the Complainant's Mother had written in her handwritten list, and then provided its explanation:¹⁵

Access 1:

On January 21, 2011, my daughter's health records were viewed 5 times by [Individual A] on the AHS' SCM database.

26. [Individual A] was a [type of physician] with AHS at the time of access, working primarily out of the [facility] in [location]. [The Complainant] presented at the [facility] on January 21, 2011 and was under the care of [Individual A]. This is noted in the "Attending Physician" column in the SCM audit that [Complainant's Mother] attached to the Notice of Inquiry.
27. While [Individual A] did access [Complainant's] health information three times in the SCM system on January 21, 2011, two other members of the care team [Individual B and Individual C] also accessed [Complainant's] health information in SCM on that date. These individuals appear in the User column of the SCM audit. [Individual B] was a registered nurse in the [facility and department] at the time of the access, and [Individual C] was a [type of health service provider] at the [facility] at the time of access. Both of these individuals were AHS affiliates at the time, and these accesses are authorized under s 27(1)(a) for the provision of health services.

¹⁵ I have assigned letters to identify each individual named by the Complainant's Mother in her handwritten list.

28. As the SCM did not begin tracking the specific information viewed by a user until 2015, there is no way to know what information was viewed.

Accesses 2 and 3:

Twice on January 31, 2011, [Individual A] viewed my daughter's health records on SCM

Twice again on June 31, 2011 [Individual A] accessed my daughter's health records on SCM¹⁶

29. While [Individual A] appears as the Attending Physician in the SCM audits, the accesses noted above were actually undertaken by two different health information management professionals.
30. On January 31, 2012 [Complainant's] health information was accessed in the SCM by [Individual D], a health information management professional at the [facility]. This access was very likely for the purpose of coding data for anonymized analytics, which are shared with Alberta Health.
31. On June 27, 2012, [Complainant's] health information was accessed in the SCM by [Individual E], a health information management professional at the [facility]. The purpose of this access was to complete a records request.
32. These individuals were AHS affiliates at the time of access and the access is authorized under s 27(1)(g) of HIA for internal management purposes.
33. As the SCM did not begin tracking specific information viewed by a user until 2015, there is no way to know what information was viewed.

Access 4:

On February 1, 2014, AHS' SCM database was accessed to view my daughter's health records by [Individual F].

34. [Individual F] is a physician that provided care to [Complainant] on February 1, 2014 at the [facility]. [Individual F] accessed [Complainant's] health information in the SCM for the purpose of providing health services. [Individual F] was an affiliate of AHS at the time of access. Access is authorized under s 27(1)(a) of the HIA.
35. As the SCM did not begin tracking specific information viewed by a user until 2015, there is no way to know what information was viewed.

¹⁶ The reference to June 31, 2011 in the Custodian's reproduction of item number 3 of the Complainant's Mother's handwritten list appears to be a typographical error since item number 3 of the Complainant's Mother's list references the access to her daughter's health information in the SCM as having occurred on June 27, 2012, and the Custodian correctly references the date June 27, 2012 in paragraph 31 of its submission.

Accesses 6, 27 and 38:¹⁷

On Nov 4, 2011 AHS' Netcare database was accessed by [Individual G] to view my daughter's records.

...

...

36. [Individual G] accessed demographic health information in Netcare PD on November 4, 2011, for [the Complainant], [Child B], and [the Complainant's Mother]. At the time of access, [Individual G] was a secretary at the [facility], and was an employee of AHS. During investigation, AHS Privacy determined that the demographic information was viewed in searching for another unrelated patient, with the same last name as [the Complainant's Mother, the Complainant, and Child B]. When trying to locate a patient by last name (versus ULI, for example) Netcare PD will bring up all relevant records, for the service provider to search through. Netcare PD only contains demographic information.
37. [Individual G] was an affiliate of AHS at the time of access. Accesses are authorized under s 27(1)(a), for the provision of health services.

Access 7:

On December 12, 2011, AHS' Netcare database was accessed by [Individual H] to view my daughter's health records at [facility]

38. [Individual H] accessed [Complainant]'s health information in Netcare on December 12, 2011. [Individual H] was a data integrity clerk employed with AHS, at the time of access. Data integrity clerks work throughout the province out of multiple facilities. Their role is to ensure the accuracy of the patient's information in Netcare, and they review patient information to determine whether remediation is required. They might access a patient's record, for example if there was a need to update an address across systems.
39. In this case, [Individual H] only viewed demographic information related to [Complainant]. [Individual H] was an affiliate of AHS at the time of access, and this access is authorized under s 27(1)(g) – internal management purposes.

¹⁷ The Custodian's reproduction of the 27th and 38th accesses identified by the Complainant's Mother in her handwritten list have been excluded as they do not involve accesses to the Complainant's health information.

Accesses 8 and 24:¹⁸

On November 8, 2012, AHS' Netcare database was accessed by [Individual I] at the [facility] to view my daughter's health records

...

40. [Individual I], like [Individual H] above, was a data integrity clerk employed with ASH at the time of access. [Individual I] worked out of the [facility] and accessed the demographic information of the Complainant and [Complainant's Mother] in Netcare PD on November 8, 2012. He reviewed Netcare PD on this date and would have been looking for anything that needed to be updated or remediated between [Complainant] and [Complainant's Mother]'s demographic information. It is likely [Individual I] was seeking to coordinate information between and [sic] parent and child file to ensure accuracy.
41. [Individual I] was an affiliate at the time of accesses, and this access is authorized under s 27(1)(g) – internal management purposes.

Access 12:

On February 1, 2014, AHS' Netcare database was accessed by [Individual J] at the [facility] to view my daughter's health records.

42. [Individual J] was an Admitting Clerk at the [facility] at the time of access. [Individual J] accessed [Complainant's] demographic information and medication profile in Netcare on February 1, 2014. [Complainant] presented at the [facility] on this date and was seen by a physician.
43. [Individual J] was an employee, and therefore an affiliate of AHS at the time of access. Access is authorized under s 27(1)(a), for the purpose of providing health service.

...

Accesses 18 and 39:¹⁹

...

On September 25, 2014, AHS' Netcare database was accessed by [Individual K] to view my daughter [Complainant's] health records.

¹⁸ The Custodian's reproduction of the 24th access identified by the Complainant's Mother in her handwritten list has been excluded as it does not involve access to the Complainant's health information.

¹⁹ The Custodian's reproduction of the 18th access identified by the Complainant's Mother in her handwritten list has been excluded as it does not involve access to the Complainant's health information.

50. [Individual K] was a [redacted] Clerk employed with AHS at the time of access. [Individual] accessed demographic health information in Netcare PD on September 25, 2014 for both [the Complainant] and [the Complainant's Mother]. In this instance a letter had been sent to [the Complainant's Mother] in relation to [the Complainant] and it had been returned to sender. Demographic information was checked to determine a correct address.
51. [Individual K] was an AHS affiliate at the time of access. Therefore, access is authorized under s 27(1)(a) - provision of health services.

[para 50] In reviewing the Custodian's submissions, I note that in Order H2021-01, the adjudicator determined that if the custodian can show a link between the complainant's information and the employee's role at the time they accessed the complainant's information, such an explanation may be sufficient even if the employee could not recall their precise actions or intentions when they accessed the information several years prior. The adjudicator stated:

[para 27] That said, the employee needn't necessarily recall that particular access of information for the Custodian to present a reasonable explanation or argument as to its authority for the access. Order H2020-04 addressed several complaints about EHR accesses that occurred from 2006 to 2012; the complaint about those accesses was made in 2014. While a significant time had passed for some of those accesses, the explanations provided by the custodian in each case were accepted. For example, an employee of the custodian accessed a complainant's EHR in 2013; the explanation that was accepted in that case was that the employee's role included administering a waitlist and that the complainant was on a waitlist for a procedure at the time (see paras. 75-77). There is no indication in the Order that the employee in question specifically recalled accessing that complainant's information on that date. The link between the employee's role of administering a waitlist and the complainant's being on a waitlist was sufficient.

[para 28] In this case, if the Custodian could show a link between the Complainant's information and the employee's role at the time they accessed the Complainant's information, such an explanation may be sufficient even if the employee could not recall their precise actions or intentions when they accessed the information several years ago. For this reason it is my view that the passage of time between the access and the Complainant's complaint is not necessarily fatal to the Custodian's ability to make its case here.

[para 51] The Custodian has explained how the location identified under the heading "Facility" in the Netcare audit log denotes the *primary* facility to which the User is affiliated.

[para 52] The Custodian has explained that it is not uncommon for AHS employees to work at multiple facilities and that where this is the case, the facility that is noted under the heading "Facility" in the Netcare audit log reflects the primary facility to which the employee is

affiliated, which may not be the facility where the employee was actually working at when they accessed the patient's health information. I accept the Custodian's explanation.²⁰

[para 53] While I understand how seeing a reference in their Netcare audit log to a facility or location they have not attended, can lead an individual to question whether their health information has been accessed without authorization, given the Custodian's explanation about the information that is recorded in the "Facility" column of the Netcare audit log, it does not automatically follow that the individual's health information has in fact been accessed without authorization.

[para 54] The Custodian has also explained how Netcare PD permits users (in this case the Custodian's employees) to search for an individual/patient to whom health services are being provided, by their last name, and to scroll through the matches that are produced in order to locate the correct individual/patient.

[para 55] As I understand the Custodian's submission, every individual whose name appears as a match to the last name search in Netcare PD, would see an access to their demographic information in Netcare PD in their Netcare audit log, simply because their name appeared as a match to the last name of the individual/patient the user/employee was searching for.

[para 56] As I understand the Custodian's position, where an employee uses Netcare PD to look up an individual/patient, using their last name, who is, has, or will be receiving a health service, the employee is viewing the demographic information produced by the broad search query as part of their job responsibilities. In these circumstances, viewing the demographic information of the individuals whose last name matches the individual/patient who is the subject of the search is a use of that information that is permitted under section 27(1)(a) of the Act. I agree that section 27(1)(a) applies in these particular circumstances.²¹

[para 57] The Complainant's Mother did not make any persuasive arguments or provide any evidence in her rebuttal submissions that would refute the submissions and conclusions reached by the Custodian following its investigation, that the accesses to the Complainant's health information by the employees of the Custodian, identified in item numbers 1 – 4, 6, 7, 8, 12 and 39 of the Complainant's Mother's handwritten list, were authorized under the Act.

²⁰ I also note that in Order F2020-12 at paragraph 27, the Custodian submitted "Although AHS is the information manager of Alberta Netcare, Alberta Health [is] responsible for the system and any changes to functionality would be its responsibility".

²¹ Where an employee of the Custodian accesses Netcare PD and views demographic information for purposes *unrelated* to their job responsibilities, as determined in Investigation Report H2018-IR-01, such use of the information is a contravention of section 27 of the Act. There is no information or evidence before me to suggest that the employee in item number 6 of the Complainant's Mother's handwritten list accessed Netcare PD and viewed the demographic information in the search results, which included the Complainant's demographic information, for purposes unrelated to their job responsibilities.

[para 58] Having reviewed all the Custodian's submissions, and the Complainant's Mother's submissions, I find the Custodian has established that the accesses to the Complainant's health information made by its employees, as Affiliates of the Custodian, which were identified in items numbers 1, 4, 6, 12 and 39 of the Complainant's Mother's handwritten list, were in compliance with section 27(1)(a) of the Act, and that the accesses to the Complainant's health information by the Custodian's employees which the Complainant's Mother identified in item numbers 2, 3, 7 and 8 of her handwritten list, were in compliance with section 27(1)(g) of the Act.

Accesses Identified in Item Numbers 5, 9, 10 and 11

[para 59] In its submission, the Custodian advised that it determined the access identified by the Complainant's Mother in item number 5 of her handwritten list by the Custodian's employee (Employee A) to the Complainant's health information in Clinibase on April 23, 2013, and the accesses identified by the Complainant's Mother in item numbers 9 (on April 5, 2013), 10 (on August 22, 2013) and 11 (on September 3, 2013) by the Custodian's employee (Employee B) to the Complainant's health information in the EHR/Netcare, were not authorized under section 27 of the Act.²²

[para 60] In item number 5 of her handwritten list, the Complainant's Mother stated that Employee A was her co-worker and that there was no reason why her co-worker needed to view her daughter's health records.

[para 61] The Custodian advised that both Employee A and Employee B were interviewed in 2016, during the investigation of this matter.²³ With respect to the access identified by the Complainant's Mother in item number 5 of her handwritten list, the Custodian stated:²⁴

79. [Employee A] accessed [Complainant's] health information in Clinibase one time on April 23, 2013. AHS Privacy determined that the information accessed by [Employee A] was demographic information only. As per the information provided above, Clinibase contains only limited health information related to admission, discharge and transfer of patients.
80. When asked, [Employee A] had no memory of having accessed [Complainant's] health information, and could not imagine why she would have done so. She acknowledged knowing [Complainant's Mother] as a work colleague, but indicated that they worked opposite shifts. AHS was not able to conclude that the access was authorized as falling within [Employee A's] work role and was therefore considered an unauthorized access as per the HIA.

²² Custodian's submission dated May 14, 2021 at paras. 19, 22, and 75 – 80.

²³ *Ibid.*, at para. 75.

²⁴ *Ibid.*, at paras. 79 – 80.

[para 62] Given the submissions of the Custodian, I find that Employee A accessed and therefore used the Complainant's health information in Clinibase on April 23, 2013 for an unauthorized purpose in contravention of Part 4 of the HIA.

[para 63] In item numbers 9, 10 and 11 of her handwritten list, the Complainant's Mother alleged that Employee B accessed the Complainant's health information in Netcare on April 5, 2013, August 22, 2013 and September 3, 2013. In her Request for Review/Complaint, the Complainant's Mother stated that Employee B "used to be roommates [sic] with my ex's cousin".²⁵

[para 64] The Custodian advised that Employee B was a clerk employed by AHS at the [location/facility] at the time of the accesses. It stated that Employee B "only has access to demographic health information in Netcare PD and did not have access to patient health information beyond demographics".²⁶

[para 65] The Custodian advised that during the investigative interview, Employee B acknowledged that the access to the Complainant's health information was not work related, and acknowledged a personal connection to the Complainant's Mother. The Custodian advised that it concluded that the Complainant's demographic health information was accessed by Employee B in contravention of section 27 of the HIA.²⁷

[para 66] Given the submissions of the Custodian, I find that Employee B accessed and therefor used the Complainant's health information in Netcare PD on April 5, 2013, August 22, 2013, and September 3, 2013, for an unauthorized purpose in contravention of Part 4 of the Act.²⁸

[para 67] Section 62(2) of the Act states that "Any collection, use or disclosure of health information by an affiliate of a custodian is considered to be a collection, use or disclosure by the custodian".

[para 68] Accordingly, pursuant to section 62(2) of the Act, I find that the Custodian contravened Part 4 of the Act when Employee A used the Complainant's health information in Clinibase on April 23, 2013, in contravention of the Act, and when Employee B used the Complainant's health information in Netcare PD on April 5, 2013, August 22, 2013, and September 3, 2013 in contravention of the Act.

²⁵ Complainant's Mother's Request for Review/Complaint Form received April 12, 2016.

²⁶ *Ibid.*, at para. 77.

²⁷ *Ibid.*, at para. 78.

²⁸ As noted herein, the definition of "health information" in section 1(1)(k) of the Act includes "registration information". Pursuant to section 1(1)(u) of the Act, and section 3 of *Health Information Regulation*, AR 70/2001, "registration information" incudes demographic information.

2. Did the Custodian fail to safeguard the Complainant's health information in Netcare in contravention of section 60 of the HIA?

[para 69] Section 60 of the Act sets out the duty on custodians to protect health information. It states:

60(1) A custodian must take reasonable steps in accordance with the regulations to maintain administrative, technical and physical safeguards that will

- (a) protect the confidentiality of health information that is in its custody or under its control and the privacy of the individuals who are the subjects of that information,*
 - (b) protect the confidentiality of health information that is to be stored or used in a jurisdiction outside Alberta or that is to be disclosed by the custodian to a person in a jurisdiction outside Alberta and the privacy of the individuals who are the subjects of that information.*
 - (c) protect against any reasonably anticipated*
 - (i) threat or hazard to the security or integrity of the health information or of loss of the health information, or*
 - (ii) unauthorized use, disclosure or modification of the health information or unauthorized access to the health information,*
- and*
- (d) otherwise ensure compliance with this Act by the custodian and its affiliates.*

(2) The safeguards to be maintained under subsection (1) must include appropriate measures

- (a) for the security and confidentiality of records, which measures must address the risks associated with electronic health records, and*
- (b) for the proper-disposal of records to prevent any reasonably anticipated unauthorized use or disclosure of the health information or unauthorized access to the health information following its disposal.*

(3) In subsection (2)(a), "electronic health records" means records of health information in electronic form.

[para 70] Section 60 requires a custodian to take reasonable steps to protect health information from foreseeable risks such as unauthorized access.

[para 71] I asked the Custodian to tell me, if it determined that any of the accesses to the Complainant's health information identified in the Complainant's Mother's handwritten list were

made by an Affiliate without authorization, what steps the Custodian had taken to comply with the requirements of section 60 of the Act and the regulations, prior to the occurrence of the unauthorized access or accesses.

[para 72] I also asked the Custodian to tell me, if it determined that any of the accesses to the Complainant's health information identified in the Complainant's Mother's handwritten list were made by an Affiliate without authorization, whether that individual received privacy training prior to the unauthorized access, and whether they signed anything acknowledging the training and/or agreeing to adhere to the Custodian's policies.

[para 73] Finally, I asked the Custodian to tell me, if it determined that any of the accesses to the Complainant's health information identified in the Complainant's Mother's handwritten list were made by an Affiliate without authorization, what steps it had taken or policies it had subsequently implemented, to comply with section 60.

[para 74] The Custodian provided the following submissions (footnotes omitted):²⁹

82. The legislation requires custodians to take reasonable mitigation steps; however it does not demand perfection. This principle was confirmed in *Alberta Health Services (Re)*, 2016 CanLII 11567 (AB OIPC) at para. 14, attached at TAB 2:

The Custodian is not obliged to maintain safeguards that will completely eliminate risks of breaches of the Act. There will be instances, such as the case here, that individuals will circumvent the safeguards.”

Notwithstanding AHS' best efforts, this is unfortunately what occurred in this case.

General Safeguards:

83. AHS has extensive safeguards in place to mitigate the risk of unauthorized use of health information. These safeguards include periodic auditing of all systems to monitor usage, and sophisticated password protection for all systems. Affiliates are only provided access to the minimum amount of health information required in their employment role.
84. AHS has a well-established and robust suite of policies governing the protection of privacy and access to health information. The AHS policies that relate to this inquiry are as follows:
 - Policy 1105 – Access to Information (Physical, Electronic, Remote)
 - Policy 1109 – Collection, Access, Use and Disclosure of Information
 - Policy 1112 – Information Security and Privacy Safeguards
 - Policy 1142 – Information Classification Policy
 - Policy 1143 – Information Technology Acceptable Use

²⁹ Custodian's submission dated May 14, 2021.

- Policy 1144 – Monitoring and Auditing of Information Technology Resources
- Policy 1177 – Privacy Protection and Information Access

All of these policies, aside from Policy 1177, were in place in 2013 when the unauthorized accesses occurred on this file. Policy 1177 was established in 2018. The policies apply to all affiliates of AHS. Attached to these submissions as TAB 3 are the current versions of the above policies.

85. Since 2016, AHS has moved to an online learning system called My Learning Link which tracks the training modules completed by each Employee in a centralized manner. The Required Organizational Learning (ROL) module related to privacy is called “InfoCare – On Our Best Behaviours” (formerly “*Collect It Protect It*”). It is an online training course which must be completed within 30 days of being hired and every three years thereafter. The training requirement includes the electronic signing of the AHS Confidentiality and User Agreement, which also must be re-signed every three years. The privacy training covers AHS privacy policies as well as the AHS Code of Conduct.
86. Attached as TAB 4 is an overview of the “On Our Best Behaviours” training course, and a description of the mandatory training requirements taken from the AHS “Insite” intranet system. Prior to 2016, privacy training was not centrally tracked in the same manner as it is today and I am informed by AHS Privacy, that information about an affiliate’s privacy training was often held with local management.
87. When a potential breach is identified, investigation and interviews are undertaken by AHS. Access for that affiliate may be suspended while the investigation is ongoing. The affiliate may be suspended from work, with or without pay, while the investigation is ongoing.
88. Where a privacy breach is confirmed, further disciplinary action may be taken against the affiliate, including but not limited to suspension from work with or without pay or termination. The determination of discipline is made on a case-by-case basis and aligns with the principles of progressive discipline and labour and employment jurisprudence. If the affiliate remains an employee, AHS may also undertake proactive or follow-up auditing of the employee’s actions to monitor their accesses. The affiliate will be reassigned privacy training and instructed to review privacy policies, practices, and the manager maintains performance management.

[para 75] The Custodian submitted that additionally, a patient’s health information can be masked in Netcare, such that any user must identify the reason for the access prior to viewing any health information, including demographic information.³⁰

³⁰ *Ibid.*, at para. 89.

[para 76] The Custodian advised that when the privacy breaches were suspected in 2016 (after the Complainant’s Mother had submitted her Request for Review/Complaint to this Office), it conducted an investigation which included interviewing Employee A and Employee B.

[para 77] The Custodian stated:³¹

Both [Employee B] and [Employee A] indicated in their 2016 interviews that they had completed privacy training and had executed a Confidentiality and Users Agreement upon hire, which would have been a requirement. AHS Privacy was not able to confirm specific information about the privacy training [Employee A] had prior to the unauthorized access in 2013, as this information was not maintained centrally until 2016. AHS was able to confirm that [Employee A] signed a Confidentiality and User Agreement in 2009. AHS Privacy was able to confirm that [Employee B] had taken privacy training in 2011 (“Information Privacy and IT Security Awareness”) prior to the unauthorized access in 2013.

[para 78] The Custodian submitted:³²

92. AHS Privacy was able to confirm that both [Employee B] and [Employee A] were required to, and did complete the InfoCare – On Our Best Behaviors (then known as *Collect It Protect It*) training module, and re-signed the Confidentiality and User agreement after the unauthorized accesses were discovered in 2016. They both would have been subject to managerial monitoring and performance management. [Employee B] faced employment based discipline.
93. [Employee B] remains employed by AHS, and as with all employees, renews privacy training every three years. [Employee A] is no longer employed by AHS.
94. Following these unauthorized accesses, the health information of [the Complainant’s Mother], [the Complainant], and [Child B] was masked in Netcare which provides an additional layer of protection. This ‘masking’ further addresses the specific risk posed by [Employee B] and [Employee A] in relation to these Complainants.

[para 79] In conclusion, the Custodian submitted:³³

95. It is submitted that the general and specific safeguards put in place by AHS were reasonable in this case, despite the unfortunate instance of unauthorized access. As such, it is submitted that AHS did not violate section 60 of the HIA.

³¹ *Ibid.*, at para. 91.

³² *Ibid.*, at paras. 92 – 94. Section 8.1(7) of *Health Information Regulation*, AR 70/2001 states that a custodian must establish sanctions that may be imposed against affiliates who breach, or attempt to breach, the custodian’s administrative, technical and physical safeguards in respect of health information. The Custodian’s submission dated May 14, 2021 indicates it has established such sanctions.

³³ *Ibid.*, at para. 95.

[para 80] The Custodian is correct that the standard required by section 60 is one of reasonableness and not perfection. As stated by the adjudicator in Order H2021-01 at paragraph 46:³⁴

[para 46] Section 60(1) requires a custodian to take reasonable steps to maintain administrative, technical and physical safeguards. This provision does not require perfection; a breach of the HIA does not necessarily mean that reasonable safeguards were not in place.

[para 81] Despite the efforts and measures taken by the Custodian, which included implementing privacy policies, providing privacy training to its employees, and having its employees sign a Confidentiality and User Agreement, on the dates noted herein, Employee A accessed the Complainant's health information in Clinibase, and Employee B accessed the Complainant's health information in Netcare PD, in contravention of the Act.

[para 82] In light of the measures the Custodian had put in place in 2013 to address its obligations under section 60, including the policies it had implemented, the privacy training it provided to its employees, and the requirement that its employees sign a Confidentiality and User Agreement upon hire, I find that the Custodian had taken reasonable steps to protect health information from unauthorized access, and complied with the requirements of section 60 in 2013 when Employee A accessed the Complainant's health information in Clinibase and Employee B accessed the Complainant's health information in Netcare PD.³⁵

[para 83] The Custodian advised that since 2016, it has moved to an online learning system which included a privacy module called "InfoCare – On Our Best Behaviours". The training course must be completed within 30 days of being hired and every three years thereafter. The training requirement includes the electronic signing of the AHS Confidentiality and User Agreement, which also must be re-signed every three years. The privacy training covers AHS privacy policies as well as the AHS Code of Conduct.

[para 84] The Custodian advised that following the discovery of the unauthorized accesses in 2016, Employee A and Employee B were required to, and did complete the InfoCare – On Our Best Behaviors (then known as *Collect It Protect It*) training module, and re-signed the Confidentiality and User agreement. The Custodian advised that they both would have been

³⁴ See too, Order H2022-01 at para. 73.

³⁵ The fact that the Custodian was not able to provide specific information about the privacy training Employee A had received prior to the unauthorized access in 2013, does not automatically lead to the conclusion that the Custodian had therefore failed to take reasonable steps to maintain administrative, technical and physical safeguards to protect health information in its custody or under its control as required by section 60. The Custodian advised that Employee A indicated in their 2016 interview that they had completed privacy training and had executed a Confidentiality and Users Agreement upon hire. The Custodian was able to confirm that Employee A signed a Confidentiality and User Agreement in 2009. Even if I were to conclude that with respect to Employee A, the Custodian did not meet its duty under section 60 because it could not provide specific information about the privacy training Employee A received, given my findings that the steps the Custodian subsequently took in 2016 to meet its duty under section 60 were reasonable, there would be nothing further I would order the Custodian to do in this case.

subject to managerial monitoring and performance management and that Employee B faced employment based discipline. Further, the Custodian advised that the Employee B remains employed by AHS, and as with all employees, renews privacy training every three years. The Custodian advised that Employee A is no longer employed by AHS. Finally, the Custodian advised that it had masked the Complainant's health information in Netcare to provide an additional layer of protection.

[para 85] In her rebuttal submission, the Complainant's Mother took issue with the fact that Employee B was still employed by the Custodian.³⁶ If the Complainant's Mother is asking that I order the Custodian to terminate Employee B's employment, I do not have the authority under the Act to make such an order. I do not have the authority to issue fines, disciplinary actions or other punitive measures.³⁷

[para 86] There is no evidence before me to indicate that either Employee A or Employee B accessed the Complainant's health information in contravention of the Act after the Custodian addressed Employee A and Employee B's actions with each of them following its investigation in 2016, and took the steps it took to protect the Complainant's health information from any further unauthorized access by Employee A or Employee B.

[para 87] I find that by requiring Employee A and Employee B to complete the *Collect it Protect It* training module and re-sign the Confidentiality and User Agreement after the unauthorized accesses were discovered in 2016, and by masking the Complainant's health information in Netcare to protect it from any further unauthorized accesses, and by implementing the additional measures in 2016 for all employees regarding privacy training, the Custodian met its obligations under section 60.

IV. ORDER

[para 88] I make this Order under section 80 of the Act.

[para 89] I find that with the exception of the one access by Employee A to the Complainant's health information in Clinibase in 2013 and the three accesses by Employee B to the Complainant's health information in Netcare PD in 2013, the remainder of the accesses by the Custodian's employees to the Complainant's health information were made in compliance with Part 4 of the Act.

[para 90] With respect to the one access by Employee A to the Complainant's health information in Clinibase on April 23, 2013, given the Custodian's concession that this access was unauthorized, I find that Employee A used the Complainant's health information in contravention of Part 4 of the Act. I also find that pursuant to section 62(2) of the Act, when

³⁶ Complainant's Mother's rebuttal submission dated May 21, 2021 at para. 2.

³⁷ This has been confirmed in other Orders of this Office (see, for example, Order H2021-01 at para. 12).

Employee A used the Complainant's health information on April 23, 2013 in contravention of part 4 of the Act, the Custodian contravened Part 4 of the Act.

[para 91] With respect to the three accesses to the Complainant's health information in Netcare PD on April 5, 2013, August 22, 2013, and September 3, 2013, given the Custodian's concession that these accesses were unauthorized, I find that Employee B used the Complainant's health information in contravention of Part 4 of the Act. I also find that pursuant to section 62(2) of the Act, when Employee B used the Complainant's health information on April 5, 2013, August 22, 2013, and September 3, 2013 in contravention of the Act, the Custodian contravened Part 4 of the Act.

[para 92] I find that the Custodian had taken reasonable steps to meet its duty under section 60 of the Act when the unauthorized accesses occurred in 2013. I find that the Custodian took reasonable steps in 2016 to meet its obligations under section 60 after determining that Employee A and Employee B had accessed the Complainant's health information without authorization. In conclusion, I find the Custodian has met its duty under section 60 of the Act in this case.

Carmen Mann
Adjudicator