ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

ORDER H2021-01

January 29, 2021

ALBERTA HEALTH SERVICES

Case File Number 004488

Office URL: www.oipc.ab.ca

Summary: An individual made a complaint to this Office under the *Health Information Act* (HIA) that their Electronic Health Record (Netcare) had been accessed by their estranged spouse (the employee) in July 2008, without authority under the *Health Information Act* (HIA). In October 2017, the Complainant requested an inquiry into the matter, which the Commissioner granted.

Prior to this complaint, the Complainant made a complaint to this Office that their estranged spouse had accessed their health information in Netcare in 2012. That complaint was made to this Office in October 2012. It was investigated by a Portfolio Officer, who issued her finding in January 2014. The Complainant requested an inquiry into that file but later withdrew that request.

In the present case, the Adjudicator determined that the Custodian provided insufficient evidence or explanation to find that the access by the employee (as affiliate) in 2008 was authorized. However, the Adjudicator was satisfied that the Custodian met its obligations under section 60(1) of the Act.

The Adjudicator found that the actions taken by the Custodian in response to the 2012 access by the same employee were sufficient as a remedy. As those actions were taken after the 2008 access at issue in this inquiry, they also addressed that contravention of the Act. The Adjudicator concluded that there were no further steps the Custodian must take.

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

Orders Cited: AB: Orders H2016-02, H2020-04, P2006-008

Cases Cited: *R. v. Sharpe*, 2001 SCC 2 at para. 33, *Rizzo & Rizzo Shoes Ltd. (Re)*, 1998 CanLII 837 (SCC), [1998] 1 SCR 27, *University of Alberta v. Alberta (Information and Privacy Commissioner)*, 2009 ABQB 112

Authorities Cited: E.A. Driedger, *Construction of Statutes*, 2nd ed. (Toronto: Butterworths, 1983), Alberta Health, *Health Information Act Guidelines and Practices Manual* (2011)

I. BACKGROUND

[para 1] On June 29, 2016, the Complainant submitted a complaint to this Office that their Electronic Health Record (Netcare) had been accessed by their estranged spouse (the employee) on July 29, 2008, without authority under the *Health Information Act* (HIA). On October 30, 2017, the Complainant requested in inquiry into the matter, which the Commissioner granted.

[para 2] Prior to this complaint, the Complainant made a complaint to this Office that their estranged spouse had accessed their health information in Netcare on January 11, 2012. That complaint was made to this Office in October 2012. It was investigated by a Portfolio Officer, who issued her finding in January 2014. The Complainant requested an inquiry into that file but later withdrew that request.

[para 3] The Custodian provided a copy of the Portfolio Officer's findings letter from January 2014, noting especially the following:

> a. AHS had advised the OIPC that:
>
> > i. it had obtained and reviewed Netcare access logs for the AHS Employee for the period January 1, 2011 to October 22, 2012 to determine the extent of the access by the AHS Employee;
> >
> > ii. it had interviewed the AHS Employee about the 2012 Access;
> >
> > iii. the AHS Employee did not recall making the 2012 Access. It was hypothesized that she likely accessed it as a part of a demonstration of Netcare while training a co-worker because it was her role at the time to mentor and train other staff;
> >
> > iv. the 2012 access was an access to Patient Demographics and it was a "view", such that no printing occurred;
> >
> > v. Patient Demographics would have included the Complainant's PHN/ULI, Name, Date of Birth, Ag, Sex, Eligibility Start Date, [Address] (primary), Address (Mailing), Home Phone Number, Work Phone Number, and Cell/Alternate Phone Number; and
> >
> > vi. as a result of the complaint to the OIPC regarding the 2012 access, AHS had reviewed the employee's Netcare access and had determined this access was no longer needed. As such, the AHS Employee's Netcare access was ended.
>
> b. AHS had taken various other steps in response to the complaint to the OIPC regarding the 2012 Access, as described on pages 5 and 6 of the Outcome Letter, namely: the AHS Employee was

required to review the AHS Privacy video, complete the AHS online privacy and security training, and review and sign the new AHS confidentiality and user agreement.

c. In addition, changes were made to the training environments for Netcare to use test users and test patient data for training.

d. As a result of AHS having taken these steps, the investigator had no further recommendations with respect to the 2012 Access.

[para 4] That complaint is not part of this inquiry; however, the findings letter provides useful information for this inquiry.

II. ISSUES

[para 5] The issues set out in the Notice of Inquiry, dated September 22, 2020, are as follows:

1. Did the Custodian use the Complainant's health information in contravention of Part 4 of the HIA (section 25)?

2. Did the Affiliate use the Complainant's health information in contravention of Part 4 of the HIA (section 28)?

3. Did the Affiliate use the Complainant's health information contrary to section 62(4) of the HIA?

4. Did the Custodian fail to safeguard health information in contravention of section 60 of the HIA?

III. DISCUSSION OF ISSUES

Preliminary issue – scope of inquiry

[para 6] In their initial submission, the Complainant provided a list of issues and questions that they wanted addressed. Some issues are substantially similar to those listed in the Notice of Inquiry. The remaining questions/issues are not matters I have jurisdiction over (such as what disciplinary action the Custodian will take).

[para 7] Some issues raised by the Complainant relate to matters within the scope of the HIA but were raised without evidence or other indication that an unauthorized action had occurred. For example, the Complainant asks if the information accessed by the employee was then used or disclosed by the Custodian. The Complainant has provided evidence, in the form of an audit log, that their information was accessed by the employee; this is the issue for the inquiry. In its initial submission, the Custodian notes that the audit log provided by the Complainant shows the access in question was an access of Patient Demographics and was a "view". It states that had the employee taken other actions (such as printing the information), that action would have been recorded in the audit log. The Complainant surmises that the employee might have taken a photo or written down the information they viewed, for subsequent use and/or disclosure. Aside from

stating that it could have happened, the Complainant did not provide any evidence or reason to believe that the information accessed by the employee was recorded and subsequently used or disclosed by them.

[para 8] In Order P2006-008, the Commissioner explained the burden of proof in relation to complaints made under the *Personal Information Protection Act* in the following way (at paras. 10-11):

> Relying on these criteria in Order P2005-001, I stated that a complainant has to have some knowledge of the basis of the complaint and it made sense to me that the initial burden of proof can, in most instances, be said to rest with the complainant. An organization then has the burden to show that it has authority under the Act to collect, use and disclose the personal information.
>
> This initial burden is what has been termed the "evidential burden". As I have said, it will be up to a complainant to adduce some evidence that personal information has been collected, used or disclosed. A complainant must also adduce some evidence about the manner in which the collection, use or disclosure has been or is occurring, in order to raise the issue of whether the collection, use or disclosure is in compliance with the Act.

[para 9] In *University of Alberta v. Alberta (Information and Privacy Commissioner)*, 2009 ABQB 112, Yamauchi J. approved this approach to the burden of proof in complaints made under the FOIP Act. The Court found (at para. 108):

> But see, Order P2006-008: ***Lindsay Park Sports Society*** (March 14, 2007)at paras. 9-21, where the OIPC said that complainants under FOIPPA do not have a legal burden, but an evidential burden. Once the complainant satisfies the evidential burden, the burden shifts to the public body to show "that it has the authority ... to collect, use or disclose personal information," at para. 20. Because of FOIPPA's structure, this Court agrees with the ***Lindsay Park*** analysis of the burden of proof and evidentiary burden.

[para 10] It is reasonable to apply this principle to complaints made under the HIA as well. As the Complainant has not adduced any evidence or reason to believe that the information accessed by the employee was subsequently used or disclosed, I am not adding either issue to this inquiry.

[para 11] The Complainant also asked (initial submission, at page 7):

> Finally, I would ask that the OIPC clarify whether it has the authority to apply fines, sanctions, disciplinary actions, or other punitive measures against the Affiliate or the Custodian, and whether the OIPC has the ability to order effective remedies, redress, compensation, or damages in favour of the Complainant.

[para 12] I do not have authority to issue fines, disciplinary actions or other punitive measures. Section 80 of the HIA sets out what the Commissioner (and I as her delegate) may order. The provision relevant to this case, are sections 80(3) and (4), which state:

> *80(1) On completing an inquiry under section 77, the Commissioner must dispose of the issues by making an order under this section.*
>
> …

(3) If the inquiry relates to any other matter, the Commissioner may, by order, do one or more of the following:

(a) require that a duty imposed by this Act or the regulations be performed;

(b) confirm or reduce the extension of a time limit under section 15;

(c) confirm or reduce a fee required to be paid under this Act or order a refund, in the appropriate circumstances, including if a time limit is not met;

(d) confirm a decision not to correct or amend health information or specify how health information is to be corrected or amended;

(e) require a person to stop collecting, using, disclosing or creating health information in contravention of this Act;

(f) require a person to destroy health information collected or created in contravention of this Act.

(4) The Commissioner may specify any terms or conditions in an order made under this section.

[para 13] This inquiry is limited to the issues listed in the Notice of Inquiry.

Preliminary issue – exercise of discretion to conduct inquiry

[para 14] In its initial submission, the Custodian asked that this Office exercise the Commissioner's discretion under section 78 of the HIA to refuse to hear this inquiry. The Custodian provides several reasons why it would be reasonable to do so.

[para 15] In this case, the Commissioner already made a determination under section 78 to conduct an inquiry. I do not have authority to amend that decision. To use a colloquial phrase, that ship has sailed. At this point, I am to decide questions of fact and law, under section 77 of the Act.

1. Did the Custodian use the Complainant's health information in contravention of Part 4 of the HIA (section 25)?

[para 16] The legislative scheme governing health information and the access of Netcare 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 Netcare and establish the authority for custodians to use electronic health information stored on this system.

[para 17] Prior to the introduction of Part 5.1, there were no statutory provisions specifically addressing the access and use of information by authorized custodians via Netcare. The 2010 amendments included section 56.5, which states that when an authorized custodian obtains health information through Netcare, this is a use of the information, rather than a collection. While the HIA did not include such a provision prior to 2010, it is consistent to treat the pre-2010 accesses also as a use of the Complainant's health information. This approach was taken by the adjudicators in Orders H2016-02 and H2020-04.

[para 18] There is no provision in the HIA enabling affiliates to collect, use, or disclose information. However, 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:

> *62(2) 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.*

[para 19] As noted above, the access of the Complainant's health information via Netcare will be considered as a use.

[para 20] With their complaint, the Complainant provided a copy of an audit log showing that the employee accessed their patient demographics information via Netcare on July 29, 2008. The Custodian does not dispute the accuracy of this audit log.

[para 21] I conclude that the employee accessed and therefore used the Complainant's health information.

2. Did the Affiliate use the Complainant's health information in contravention of Part 4 of the HIA (section 28)?

3. Did the Affiliate use the Complainant's health information contrary to section 62(4) of the HIA?

[para 22] The discussion of these issues is intertwined; I will therefore consider them together.

[para 23] Section 28 of the HIA 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 24] Section 62(4) provides as follows:

> *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.*

[para 25] In its initial submission, the Custodian states that it interviewed the employee regarding the 2008 EHR access. The employee has no recollection of the access or the purpose of the access. The Custodian argues that it has been many years since the access, and that its ability to respond has been significantly prejudiced by this passage of time. It states (initial submission, at paras. 22-24):

> As the AHS employee has no recall of the 2008 Access, AHS' ability to respond to this Inquiry has been significantly prejudiced. AHS is unable to lead evidence regarding the purpose of that access. As

> a result of the absence of evidence, AHS is unable to respond to the issues of whether the use was permitted by section 25 of the HIA, whether the use was in accordance with the AHS Employee's duties to AHS as required by section 28 of the HIA, whether the AHS employee's use of the health information was contrary to section 62(4) of the HIA, or whether AHS failed to safeguard health information in accordance with section 60 of the HIA.
>
> AHS submits that, where the only evidence available to the OIPC is that an access occurred, it should not be presumed that the access was a breach of the HIA. Such presumption, especially where there has been a loss of evidence that is significantly prejudicial to the custodian, would be offensive to the expectations of fairness. It also places the Commissioner in the unenviable position of attempting to make a determination of mixed fact and law in the absence of an evidentiary basis.
>
> In the alternative, AHS submits that the determination of the purpose for the 2008 Access should be based on the same theory as the purpose of the 2012 Access, which has previously been addressed.

[para 26] I understand the Custodian's concern about the loss of evidence. Eight years had passed between the access at issue, and the date of the Complainant's complaint to this Office about that access. It would be undoubtedly difficult for most individuals to recall an event so far in the past.

[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 29] In its submissions, the Custodian has not provided an explanation of the employee's role in 2008, or why that role would involve accessing the Complainant's information. However, the Custodian has suggested that the employee's 2008 access was for the same purpose as the 2012 access "which has previously been addressed" (initial submission, at para. 24).

[para 30] The Custodian did not directly discuss the 2012 access but it did provide a copy of the Portfolio Officer's findings letter. That letter sets out the relevant facts, the Custodian's explanation of the 2012 access and its arguments regarding its authority.

[para 31] Usually findings letters from portfolio officers (now Senior Information and Privacy Managers) are not considered in an inquiry. In this case, the Custodian has provided the findings letter from the previous review, presumably as a 'shortcut' way of providing me with the same information it provided the Portfolio Officer during her review of the 2012 access. I will consider the information outlined in the findings letter, as well as the discussion of the Custodian's position in that case.

[para 32] The 2012 access of the Complainant's information was conducted by the same employee (the Complainant's estranged spouse). The Portfolio Officer's findings letter outlined the following facts:

> AHS interviewed the employee about the single access. According to AHS the employee did not recall making the access to the Complainant's information but continued to explain that the access was likely part of a demonstration of Netcare while training a co-worker because it was part of her role at the time to mentor and train other staff. The employee stated that she already knew the information and gained no additional information by the same information via Netcare.
> …
> AHS confirmed that the employee in question is a secretary within the Calgary Zone of AHS and at the time of the access the employee's Netcare access (access to the system overall) was appropriate and necessary for her role. The employee received training on the use of Netcare and AHS privacy training. AHS also confirmed that the employee was not involved in the provision of a health service to the Complainant at the time the access was made.
>
> AHS confirmed that part of the employee's responsibilities at the time the access was made was to train new staff. Therefore, it is AHS's position that the use of Complainant's demographic information was in accordance with section 27(1)(e) of the HIA. However, AHS also stated that the use of Netcare for the purposes described in this complaint was not in accordance with the Netcare Information Exchange Protocol (IEP). The IEP establishes the specific rules for the collection, use, and disclosure of information through the Alberta Netcare Electronic Health Record (Alberta Netcare).

[para 33] The findings letter further states:

> AHS explained that the employee accessed the basic demographic information of the Complainant. This included the Complainant's PHN/ULI, Name, Date of Birth, Age, Sex, Eligibility Start Date, Address (Primary), Address (Mailing), Home Phone Number, Work Phone Number, and Cell/ Alternate Phone Number.
>
> The employee does not recall who she was training at the time of the access but assumed that the access would have been part of training a co-worker on the use of Netcare. AHS explained that the employee assumed that using the Netcare information of someone she already knew was preferable or less intrusive than using information of persons unknown to her for training purposes.

[para 34] Section 27(1)(e) of the HIA states:

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

…

(e) providing for health services provider education;

[para 35] This provision does not appear to have been considered in previous Orders of this Office. The *Health Information Act Guidelines and Practices Manual* (Guidelines), published by Alberta Health, describes the purpose of this provisions as follows (at pages. 203-204):

> This provision enables a custodian to use individually identifying health information to train health services providers and students through various levels of teaching and need to know environments. This use must still respect the principle of highest level of anonymity possible. It may not be necessary, for example, to use individually identifying health information in a case study presented in a non-clinical context.
>
> For example students involved with care and treatment of specific patients on a hospital unit would have access to individually identifiable health information for only those specific patients. Students would not be provided access to health information about other patients on that unit. For students within a classroom environment, practical treatment and care scenarios would include anonymized individual/patient health information not individually identifiable information.

[para 36] While this guidance is not binding, it is helpful in determining the scope of section 27(1)(e). It is also consistent with section 58 of the HIA, which states:

> *58(1) When collecting, using or disclosing health information, a custodian must, in addition to complying with section 57, collect, use or disclose only the amount of health information that is essential to enable the custodian or the recipient of the information, as the case may be, to carry out the intended purpose.*

[para 37] The modern approach to statutory interpretation is as follows:

> …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 (*Rizzo & Rizzo Shoes Ltd. (Re)*, 1998 CanLII 837 (SCC), [1998] 1 SCR 27 at para. 21 and *R. v. Sharpe*, 2001 SCC 2 at para. 33, each quoting E.A. Driedger, *Construction of Statutes*, 2nd ed. (Toronto: Butterworths, 1983), p. 87).

[para 38] Reading section 27(1)(e) in the context of section 58, and the HIA as a whole, indicates that identifying health information can be used for training or education purposes only if *that particular* health information is essential to that training or education. As discussed in the *Guidelines*, this would arise in a hospital or similar setting where students are involved with treating particular patients. Otherwise, anonymized information is to be used instead.

[para 39] According to the Portfolio Officer's findings letter, the employee surmised that they accessed the Complainant's health information to train someone else, because it seemed less intrusive than accessing a stranger's health information. In other words, there is no indication that the *Complainant's particular* information was essential or even relevant to the training being conducted.

[para 40] In my view, section 27(1)(e) would not authorize the employee's access of the Complainant's health information in 2008, assuming that is why they did access the information.

[para 41] The Custodian has not provided any alternative reasons for the employee's 2008 access and none seem apparent from the submissions before me. Therefore, while I acknowledge the difficulties the passage of time has created for the Custodian in providing submissions in this case, the information before me does not suggest any authority for the 2008 access of the Complainant's health information from Netcare.

[para 42] A discussed at paragraph 9 of this Order, once the Complainant satisfies the evidential burden of showing the access occurred, the burden shifts to the Custodian to show that it was authorized. The Custodian has not met this burden; as such, I cannot conclude that the access was done with authority under the HIA.

[para 43] As stated in Order H2020-01, access to Netcare information by an affiliate without any authority to do so is a contravention of section 62(4)(a) of the Act. An affiliate can access health information only for the purposes for which the Custodian can access it (at para. 6). As there was no authority for the Custodian to access the Complainant's health information as it did, the employee (as affiliate) likewise did not have authority. It follows that the employee did not comply with section 62(4).

[para 44] The Custodian's submissions also indicate that the employee's access of the Complainant's health information was contrary to the Custodian's policies (for example, the Protection and Privacy of Health and Personal Information policy provided with the Custodian's rebuttal submission). As such, the access was in contravention of section 64(2)(b) of the Act, as well as section 28, which requires affiliates to use health information only in accordance with their duties to the custodian.

4. Did the Custodian fail to safeguard health information in contravention of section 60 of the HIA?

[para 45] Section 60 of the HIA requires a custodian 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 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 47] In their rebuttal submission, the Complainant states that the Custodian did not have appropriate safeguards in place as it failed to discover the employee's 2008 access of their health information "in a timely fashion" (rebuttal at para. 22). The Complainant states that the Custodian did not find this 2008 access when it investigated the same employee's access in 2012. The Complainant seems to be arguing that the Custodian failed to properly or fully investigate the 2012 access and that this failure weakens the safeguards put in place to protect health information from unauthorized access.

[para 48] When investigating the 2012 access, the Custodian states that it reviewed the employee's audit logs for January 2, 2011 to October 22, 2012, as well as the audit logs showing access to the Complainant's health information in Netcare for the same period. No other improper accesses were found in that time period. The 2008 access was therefore not noted at that time.

[para 49] With its rebuttal submission, the Custodian provided copies of relevant policies that were in force in 2008. These policies are all classified as "Information Security and Privacy" policies. They set out the obligation of employees (and contractors) to review and follow the rules set out by the Custodian regarding the use of IT resources. While these policies are, in my view, inferior to the more current policies provided by the Custodian with its initial submission, they do set out appropriate obligations regarding patient information and the proper use of IT resources (including Netcare). They require users (including employees) to have training in information security and privacy, and to sign confidentiality agreements. Policy 1487 specifically states that the use of clinical databases for training purposes is to be avoided (section 7.2).

[para 50] In my view, the Custodian had reasonable security arrangements to avoid the type of unauthorized accesses conducted by the employee. That an employee failed to follow the Custodian's rules does not mean that the Custodian did not take reasonable steps to maintain the security of the Complainant's information. That the employee committed the unauthorized access more than once also does not necessarily negate the reasonableness of the Custodian's steps. Had there been evidence that this type of unauthorized use of Netcare was commonplace, or that the Custodian ought to have known it was occurring, I may have concluded that the safeguards put in place by the Custodian to protect against unauthorized access were ineffectual in this regard. The employee in question here conducted the unauthorized access twice over a four year span; this is not sufficient for me to conclude that the behaviour was commonplace such that the Custodian's safeguards were ineffective.

[para 51] Further, that the Custodian did not identify the 2008 breach before it was identified by the Complainant does not meant that it failed to maintain appropriate safeguards. The Custodian's explanation of why it did not identify the 2008 access in the course of its investigation into the 2012 access is reasonable. The Custodian reviewed the employee's accesses, and all accesses of the Complainant's health information in Netcare, over a two-year span; it did not locate any additional instances of unauthorized access. I am not satisfied that the investigation undertaken by the Custodian into the 2012 access was deficient such that it would undermine the safeguards taken by the Custodian.

[para 52] It should also be noted that, as a result of the investigation into the 2012 access, the Custodian revoked the employee's access to Netcare (discussed below). This effectively ensured that the employee would not undertake such actions again in the future.

Remedies already undertaken by the Custodian

[para 53] The Portfolio Officer's letter of finding sets out the actions taken by the Custodian to respond to the 2012 access.

[para 54] The Custodian took steps to stop the practice of employees using health information in Netcare for training purposes. According to the findings letter,

> … Alberta Netcare has continued to improve their training materials and enhance their training environment which includes test users and test patient data to be used for new Netcare users and available as a refresher for existing users. AHS Information Privacy and IT Security Awareness training has been updated (training video etc.) to include clear direction that employees are never to access their own, their families or friends information for unauthorized purposes. This training is required annually for all employees. AHS continues to communicate to users that proactive audits are being conducted on their access.

[para 55] The Custodian also reviewed the employee's need to access Netcare, and determined that their access was no longer necessary for their work duties. Therefore, they no longer have access to Netcare. The Custodian confirmed in its initial submission that the employee's access to Netcare has not been reinstated.

[para 56] The Custodian also confirmed that the employee was required to complete additional privacy training after the 2012 access.

[para 57] Had the access at issue in this inquiry occurred *after* the 2012 access, I would have reason to doubt the efficacy of the Custodian's actions taken in 2012. However, the access in this case occurred four years prior to the 2012 access. I have no reason to believe that the Custodian's actions taken in response to the 2012 access were inadequate or otherwise did not 'stick'.

[para 58] In my view, the actions taken by the Custodian in response to the 2012 access were sufficient as a remedy in that case. In the case here, the issues are very much the same, with the access being conducted by the same employee, prior to the steps taken by the Custodian. Therefore, as the actions taken to remedy the 2012 access were sufficient, they are also sufficient to remedy the issue here. As such, I see no reason to require the Custodian to undertake the same steps again.

IV. ORDER

[para 59] I make this Order under section 80 of the Act.

[para 60] I find that the Custodian has provided insufficient evidence or explanation to find that the access by the employee (as affiliate) in 2008 was authorized.

[para 61] I find that the Custodian met its obligations under section 60(1) of the Act.

[para 62] The actions taken by the Custodian in response to the 2012 access by the same employee/affiliate are sufficient; as such, there is nothing for me to order.

_____

Amanda Swanek
Adjudicator