ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

ORDER H2016-02

January 26, 2016

ALBERTA HEALTH SERVICES

Case File Number H5739

Office URL: www.oipc.ab.ca

Summary: In submissions to the inquiry, the Custodian conceded that the Complainant's health information had been used without authorization. The Adjudicator required the Custodian to put in place safeguards that protected the Complainant's health information from a specific identifiable risk.

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

Authorities Cited: AB: Investigation Report F2013-IR-03/P2-13-IR-01/H2013-IR-02

I. BACKGROUND

[para 1] The Complainant had requested disclosure logs for her Alberta Electronic Health Records (Netcare). She discovered that an individual (the Affiliate) had reviewed her health information. The Complainant knew the Affiliate and also knew that this person had no reason to review information in her records. The Complainant believes that the Affiliate may have obtained information in the Complainant's records and used it to contact the Complainant's employer and another individual.

[para 2] An investigation into this matter did not resolve concerns of the Complainant and an Inquiry was directed.

II. ISSUES

1. Did the Custodian (or affiliate) use the Complainant's health information in contravention of section 25 of the *Health Information Act* (the Act)?

2. Did the Custodian fail to safeguard health information in contravention of section 60 of the Act?

III. DISCUSSION OF ISSUES

1. Did the Custodian (or affiliate) use the Complainant's health information in contravention of section 25 of the *Health Information Act* (the Act)?

[para 3] Section 25 states:

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

[para 4] With respect to Issue 1, the Custodian concedes that a breach of section 25 occurred by an affiliate of the Custodian. The following submissions were made on this issue:

> 1. As a result of a complaint from an affected individual (the Complainant) received by AHS Privacy on September 4, 2013, it was determined that on April 11, 2013 a Registered Nurse at the Queen Elizabeth Hospital in Grande Prairie accessed an individual's health information, on one occasion, in Netcare with no need to know.
>
> 2. When interviewed by the Responsible Manager, the employee was remorseful and took full responsibility for the incident. The employee admitted to improperly accessing the Complainant's health information with Alberta Netcare on one occasion. The information accessed included the Complainant's demographics and two patient reposts. The employee used the Complainant's phone work number contained from Netcare to contact the Complainant's place of employment in order to lodge a complaint against the Complainant. The following day the employee was remorseful and again contacted the employer to apologize and withdraw the complaint. No evidence of any harm to the Complainant was identified for this action. The employee has stated and audit logs confirm that no information was printed and no copies were made of any information from Netcare. A review of the employee's access in Meditech and Netcare revealed no other improper accesses.
>
> …
>
> 10. In accordance with section 28 of HIA 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. The unauthorized access by the employee was a breach of section 28. Since the employee is an affiliate of AHS and under section 62(2) of the HIA a use of health information by an affiliate is a use also by the custodian AHS concedes that on this occasion it is in contravention of HIA.

[para 5] The submissions of both parties indicate to me the Affiliate was the only person who used the Complainant's health information without authorization.

[para 6] Given the Custodian's concession on this issue, I find that an affiliate of the Custodian used the Complainant's health information in contravention of section 25 of the Act. Accordingly, I also find the Custodian was in contravention of section 25 of the Act.

2. Did the Custodian fail to safeguard health information in contravention of section 60 of the Act?

[para 7] Section 60 of the Act 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.*

[para 8] The Custodian submitted Part B and E of an Organizational Privacy Impact Assessment (PIA) prepared by Alberta Health Services as required by section 64 of the Act. The PIA is dated January 24, 2012. It was reviewed by the Commissioner on

March 30, 2012. Parts B is entitled Organizational Privacy Management and Part E is entitled Policy, Procedures and Attachments.

[para 9] The PIA outlines the policies of the Custodian regarding security of the health information. Training and awareness procedures include compulsory training for all employees and affiliates prior to access to information systems.

[para 10] The Custodian also provided me with copies of three of its Information Management and Technology Policies (1112 – Collection, Access, Use and Disclosure of Information, 1108- Delegation of Authority and Responsibilities for Compliance with FOIPP and the HIA, and 1143 – Information Security and Privacy Safeguards). These policies specifically limit the collection and use of information by authorized persons, to be done only in accordance with the Act and only in the performance of their duties to the Custodian. Further, the policies provide for education, training and auditing of compliance with policies. There are policies that outline reporting and discipline for breaches of the policies.

[para 11] In rebuttal submissions, the Custodian also provided me with copies of policy 1144 which governs monitoring and auditing of IT resources. This policy outlines the technical safeguards to unauthorized access. All of these policies were in place when the Affiliate used the Complainant's health information without authorization.

[para 12] These policies indicate to me that the Custodian has considered that there is a risk that its employees and affiliates may use or access health information without authority. The policy measures outlined to me are intended to protect against this unauthorized use or access.

[para 13] The Act requires "reasonable steps" to maintain safeguards. The Custodian directed me to para 20 of Investigation Report F2013-IR-03/P2-13-IR-01/H2013-IR-02:

> Taking reasonable measures to protect against risk implies that the respondent need to analyse what kinds of risks may affect personal and health information. In performing this analysis, it is important to consider measures to mitigate these risks. Each law includes the concept of reasonableness, which means that mitigation strategies do not need to be perfect. Information security and breaches may still occur even when reasonable safeguards have been implemented (my emphasis).

[para 14] 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.

[para 15] I find that the Custodian, through its PIA and implementation of policies has taken reasonable steps to maintain safeguards to generally protect the confidentiality of the Complainant's health information and to generally protect against reasonably anticipated unauthorized use, disclosure or access to that information.

[para 16] While I have found that the Custodian has taken reasonable steps to safeguard the Complainant's health information generally, I cannot say that once it determined that there was a specific risk from an identifiable individual (the Affiliate), reasonable steps were taken to mitigate that risk.

[para 17] In this case, it is clear that the Affiliate breached provisions of existing policies. I have been informed that the Affiliate was subject to discipline by the Custodian. I was not given details of this discipline, and whether it was directed at mitigating the risk of unauthorized use of the Complainant's or others' health information by the Affiliate.

[para 18] I was also told that:

> The employee has stated and audit logs confirm that no information was printed and no copies were made of any information from Netcare. A review of the employee's access in Meditech and Netcare revealed no other improper accesses.

[para 19] I was not given any detail regarding the review of the Affiliate's access in Meditech and Netcare. For example, I was not told the dates that the review period covered, nor was I told that there would be further reviews.

[para 20] The Complainant also reported the Affiliate to her governing professional body. The decision of that body was provided to me by the complainant. In its decision, the Affiliate's professional governing body found the Affiliate guilty of unprofessional conduct and imposed sanctions. The sanctions imposed are not related to the Affiliate's access to the Complainant's health information except in a general way. The Affiliate was ordered to complete modules on ethics and privacy.

[para 21] The Custodian submitted correspondence that shows that upon receipt of the Complainant's request, her Netcare information was "masked". The same correspondence indicates that "masking" provides an additional layer of privacy to that information. As I understand it, "masking" applies to all employees and affiliates of the Custodian and not only this Affiliate.

[para 22] I also learned from correspondence that the Affiliate was required by the Custodian to issue letters of apology to both the Complainant and her employer.

[para 23] I was not given a copy of the letter of apology to the Complainant's employer. The letter of apology to the Complainant indicates that the Affiliate viewed the Complainant's health information for no reason. It further indicates that the information was not copied. The Affiliate indicates that the personal information was not shared with anyone and that she has not viewed the Complainant's file since the incident and will not do so in the future.

[para 24] The facts stated in this apology differ somewhat from the Affiliate's agreed statement of facts presented to her governing body. In that decision, the governing body stated that the Affiliate admitted to the following:

> …That while employed as a [professional health care provider] at the [named hospital],
> 1. On or about April 11, 2013, she breached confidentiality when she accessed the clinical records of [the Complainant] when she was not authorized to do so and for her own personal use.
> 2. On or about June and/or July 2013, she inappropriately
>
> a. Made accusations of a personal nature about [the Complainant] with [the Complainant's] manager at her employer [named employer], in an attempt to discredit [the Complainant] with her employer;
> b. Told [the Complainant's] manager that she is a [professional health care provider], and she does not recall, but may have made remarks implying that if he did not cooperate,
>
> i. she would try to discredit [the Complainant's employer] with her co-workers;
> ii. she would try to get her employer to move their business away from [the Complainant's employer]

[para 25] It would appear from the facts before the discipline panel, the Affiliate agreed that the access was not for "no reason", but for her personal use. Any such future use by the Affiliate should certainly be considered a major risk for the Complainant's and others' health information.

[para 26] I learned from the same correspondence referred to in para. 22 that:

> Proactively our Information & Privacy Office and Human Resources Employee Development to issue (*sic)* a program for annual continuing education for <u>all AHS employees</u> and refresh of a resigning of the AHS Confidentiality and IT User Agreement for staff during the performance appraisal process so staff are aware of their obligations to collect, use and disclose health information in accordance with their roles and responsibilities and not for personal use (my emphasis).

[para 27] I cannot see how this mitigates the specific identifiable risk that the Affiliate presents to the Complainant and others. I find that the Custodian has not demonstrated how it will protect against any reasonably anticipated unauthorized use, disclosure or access to the Complainant's or others' health information by the Affiliate.

[para 28] The Complainant, in attachments to her request for Inquiry and her in submissions to the Inquiry has made it clear that only one resolution of this matter would satisfy her. She states:

> My only acceptable resolution is to have her [the Affiliate] fired – she stole – she lied and she got caught.

[para 29] The Complainant seeks a resolution that is not within my jurisdiction to order. She also believes that I have authority to order text and phone records in order to find that the Affiliate had a malicious motive when accessing the Complainant's health information. I do not have the jurisdiction to order text and phone records of the Affiliate.

[para 30] I am limited in my jurisdiction by the provisions of sections 80(1) and (3) of the Act in this Inquiry. Those sections 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.*

[para 31] The Custodian has submitted "No evidence of any harm to the Complainant was identified for this action."

[para 32] I accept the Complainant's submissions as evidence of the harm she has suffered as a result of the Affiliate's actions. The Complainant describes feeling vulnerable and helpless. She is concerned that her health information is not secure and may be subject to further unauthorized access, use and disclosure. She relates she is fearful of seeking emergency medical attention at the Affiliate's hospital.

> …what she did was no different than stealing a wallet and information but not private health information. There are things on my file that I do not want nor should have ever had to worry that it was stolen – she violated me just like a rapist – I feel vulnerable and helpless and Alberta Health Services and the QEII have left me feeling this way…I have not went for physical in over 2 years because I know my information and any prescription I take is on your secure system that [the Affiliate] can look at…

[para 33] The policies that the Custodian had in place when the breach occurred are the same policies in place today. Now that the Custodian is aware that there is a specific risk to the Complainant's health information, there should be some mechanism in place to ensure that the Affiliate is in compliance with those policies and specifically in compliance with the policies in relation to the Complainant. It is not clear to me that the Custodian has effective safeguards in place to mitigate the specific risk that the Affiliate poses to the unauthorized use, disclosure or access to the Complainant's or others' health information and I will order that the Custodian develop those safeguards.

V. ORDER

[para 34] I make this Order under section 80 of the Act.

[para 35] I order the Custodian to comply with its duty under section 60 and take steps to safeguard the Complainant's health information against the risk that the Affiliate will use or disclose the health information she accessed from Netcare without authority. I also order the Custodian to take steps to ensure that the Affiliate will not access, use or disclose the health information of anyone else without authority. If the Custodian has already taken these steps, I order it to inform the Complainant and me.

[para 36] I further order the Custodian to notify me in writing, within 50 days of being given a copy of this Order that it has complied with the Order.

_____

Neena Ahluwalia Q.C.
Adjudicator