ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

ORDER F2020-32

October 29, 2020

ALBERTA HEALTH SERVICES

Case File Number 007466

Office URL: www.oipc.ab.ca

Summary: The Complainant made an access request to Alberta Health Services (the Public Body) for information regarding a complaint she had made. The Public Body located responsive records, severed information from them and sent them to the Applicant by regular mail. The Applicant did not receive the record package. The Applicant complained to the Commissioner that the Public Body had not taken reasonable steps to ensure the security of her personal information when it mailed the records to her, in contravention of section 38 of the FOIP Act.

The Adjudicator found that although the package went missing, the Public Body had taken reasonable steps to ensure the security of the Complainant's personal information.

Statutes Cited: AB: *Freedom of Information and Protection of Privacy Act*, R.S.A. 2000, c. F-25, ss.1, 38, 72, 83; *Personal Information Protection Act*, S.A. 2003, c. P-6.5

Authorities Cited: AB: Orders P2012-02, F2013-11, F2014-19

Cases Cited: *Workers' Compensation Board v Alberta (Information and Privacy Commissioner)*, 2014 ABQB 99 (CanLII)

I. BACKGROUND

[para 1] On December 15, 2017, the Commissioner received the Complainant's complaint that the Public Body had disclosed her personal information in contravention of the FOIP Act when it sent her a disclosure package that failed to arrive at her address.

[para 2] The Commissioner authorized a senior information and privacy manager to investigate and attempt to settle the matter. At the conclusion of this process, the Complainant requested an inquiry.

II. ISSUE: Did the Public Body meet its obligations as required by section 38 of the *Freedom of Information and Protection of Privacy Act* (protection of personal information)?

[para 3] Section 38 of the FOIP Act states:

> *38 The head of a public body must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction.*

[para 4] In Order P2012-02, the Adjudicator interpreted section 34 of the *Personal Information Protection Act* (PIPA). Section 34 of PIPA is similar to section 38 of the FOIP Act, and states:

> *34 An organization must protect personal information that is in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.*

[para 5] The Adjudicator stated:

> To be in compliance with section 34, an organization is required to guard against reasonably foreseeable risks; it must implement deliberate, prudent and functional measures that demonstrate that it considered and mitigated such risks; the nature of the safeguards and measures required to be undertaken will vary according to the sensitivity of the personal information (Order P2006-008 at para. 99).

[para 6] In Order P2012-02, the Adjudicator determined that "sensitivity" refers to the potential consequences to the individual if the individual's personal information is disclosed. For example, whether the individual whom the information is about could suffer harm as a result of the disclosure, or could become the victim of identity theft, are relevant questions when determining whether information is sensitive.

[para 7] In Order F2014-19, the Adjudicator noted:

> Section 38 addresses whether a public body has made reasonable security arrangements to safeguard personal information; it does not directly address situations in which a breach is alleged but the safeguards were reasonable. In other words, it is possible for a public body to have made

> reasonable security arrangements and yet personal information can be accessed, used, disclosed or destroyed in an unauthorized manner. For example, a "rogue" employee who is appropriately authorized to access information may access the information for unauthorized purposes. This is essentially the situation alleged by the Complainant. In such a case, it is not clear that section 38 is contravened.

[para 8] Like section 34 of PIPA, section 38 of the FOIP Act imposes a duty on a public body to make reasonable security arrangements to protect personal information. The Adjudicator in order F2014-19 accepted that a public body may have reasonable security arrangements in place even though information is the subject of unauthorized collection, use, or disclosure. I agree with her reasoning. As I noted in Order F2013-11, in my view, a public body will have met the duty under section 38 if it demonstrates that deliberate, prudent, and functional measures have been adopted to guard against, or mitigate, a foreseeable risk. The extent to which security measures are necessary would then correlate to the sensitivity of the information.

[para 9] The Applicant states:

> August 24, 2016 I spoke to [the SIPM] once again. [The SIPM] spoke to [the FOIP Coordinator] who verbally told her the CD format of the report was sent via Canada Post May 06, 2016 [to] the appropriate address. There was no tracking of the document with Canada Post. I was concerned with the contents of my records gone missing. [The SIPM] said there was nothing she could do to track it now. According [to a Court] ruling sending [FOIP] records via General Delivery Canada Post is adequate. [The SIPM] also stated because their program is publicly funded it would add more expense to track or courier their reports.
>
> I was informed another CD format of records will now be couriered with the original covering letter sent on May 06, 2016. I should expect to get my CD format records by Friday, August 26, 2016.
>
> I am concerned that [the Public Body's FOIP Coordinator] is not being overly concerned with my personal information going missing in documents they prepared. [The SIPM] spoke to [the FOIP Coordinator] and had no explanation as to why I had not received my records as yet. They should have the same accountability to assuring personal records are secure and safe as do the employees working for Alberta Health Services.
>
> This is a very serious matter when my personal information goes missing. Who knows who has my original CD form report? They could pass it on to the media?

[para 10] The Applicant is concerned that the Public Body did not take all reasonable measures to protect her personal information from unauthorized disclosure when it sent the disclosure package to her. She is concerned that the contents have gone missing and could be accessed by anyone.

[para 11] I agree with the Complainant that her personal information within the terms of section 1(n) of the FOIP Act was contained in the disclosure package, as the records she requested were about a complaint she had made and its disposition by the Public Body. However, the information is not necessarily sensitive personal information, as described in Order P2012-02, as it is not the kind of information that could be used to steal the Complainant's identity or to harm her in some similar way. I acknowledge that

the Complainant is concerned that the information in the records could be disclosed to the media; however, I am unable to find this to be a likely outcome on the evidence before me. In this case, the Public Body severed information from the records, with the result that many details of the complaint were not included in the disclosure package. In making this finding I do not mean to say that the loss of the Complainant's personal information is insignificant, only that the personal information does not necessarily require heightened security measures, such as when the personal information consists of a credit card number or social insurance number.

[para 12] The Public Body argues the following:

> From the Applicant's Request for Review/Complaint form, it appears the Applicant is arguing that AHS failed to meet its obligations under section 38 of FOIP by using a form of transmittal in response to her FOIP Request which failed to include tracking information to protect against the loss of records, which could therefore lead to unauthorized access, use or disclosure of personal information. Of note, there are no claims that the Applicant's personal information was actually accessed or used unlawfully by AHS or any third party, but only that the package containing the Applicant's personal information never arrived by regular mail.
>
> […]
>
> The issue of whether or not the sensitive nature of personal information contained within a disclosure package requires more secured methods of transmittal than those provided for in section 83(1)(a) has been addressed by the Alberta Court of Queen's Bench. The Court determined that requiring delivery by means which utilize tracking information or other security measures is unreasonable to the extent that such a requirement would preclude regular prepaid mail in cases where registered mail is not expressly required by statute.
>
> *Workers' Compensation Board v Alberta (Information and Privacy Commissioner)*, 2014 ABQB 99, at paras 56 - 59, 17.
>
> *FOIP* does not require delivery by registered mail. Consequently, AHS' transmittal of the FOIP Response by way of regular prepaid mail represents a reasonable and statutorily permissible method of transmittal under *FOIP*.

[para 13] The Public Body argues that public bodies may send personal information using regular mail in accordance with section 83, unless a statute provides otherwise. It relies on *Workers' Compensation Board v Alberta (Information and Privacy Commissioner)*, 2014 ABQB 99 (CanLII) for this proposition. In *Workers' Compensation Board*, the Court of Queen's Bench interpreted an order of this office that a public body use secure, traceable means to send sensitive personal information in the future, as one requiring such information to be sent by registered mail. The Court concluded the order was unreasonable to that extent. The Court noted that the service and notice provisions in section 83 of the FOIP Act allowed service and notice of documents to be provided by regular mail rather than registered mail; as a result it was unreasonable to order public bodies to send personal information by other means, absent express statutory requirements to send mail a particular way.

[para 14] I take note that regular mail, when it is prepaid and properly addressed, is a secure and reliable means by which to send information, including sensitive

information. In addition, if a public body has a system by which staff members document having sent information and the date on which it is sent, regular mail is also a means by which a public body can trace when and whether information has been sent. Similarly, email and fax also constitute secure and traceable means by which to send personal information when the correspondence is properly addressed.

[para 15] The Public Body states:

> The FOIP Response was sent under cover letter to the attention of the Applicant at the Mailing Address, and was posted for delivery via regular pre-paid mail.

The Public Body provided a copy of the cover letter. The letter contains the correct address of the Complainant.

[para 16] I do not interpret the Court in *Workers' Compensation Board* as suggesting that a public body need not take measures to prevent unauthorized disclosure of personal information it sends through regular mail. On the contrary, the Court upheld the aspect of F2013-11 requiring the Workers' Compensation Board to take reasonable measures to address correspondence so as to ensure that the appropriate party receives correspondence containing personal information. Accordingly, I asked the Public Body about its processes for sending out disclosure packages. It stated:

> It is AHS' belief that the disclosure package was mailed to the Applicant on May 6, 2016. The response letter is dated May 6, 2016, and disclosure packages are mailed on the date indicated on the response letter. In addition, the "Recommendation for Release" document used internally to review and approve AHS' responses prior to the disclosure of records was completed on May 6, 2016 for this request (see enclosed).
>
> Further, the time noted on an internal email between the advisor who processed the response, and the AHS Director, FOIP & HIA Access Services at that time, shows that the Recommendation for Release was approved and sent to the Advisor at 11:21 am on May 6, 2016 (see enclosed email chain). Therefore, the Advisor received approval early on May 6, 2016 and had the remainder of the day to prepare and issue the response for mailing. Upon completing the disclosure package, the advisor would have placed it into the "Outgoing Mail" basket to be mailed at the end of the day by an Administrative Assistant.
>
> We note that May 6, 2016 was a Friday. It is unlikely that the Advisor who processed this request would have created the response letter on that date yet fail to issue it at that time. As the deadline to respond was May 27, 2016, if the Advisor didn't have time to prepare the response package on the Friday, he would likely have left its preparation until the following Monday May 9, 2016, and mailed it at that time with a corresponding response letter dated May 9, 2016 given the significant period of time remaining to respond before the deadline.
>
> Further, the Advisor who completed the processing of this request has completed over 700 access requests over a sixteen (16) year career with AHS (and its predecessors). Not once has it been alleged that he forgot or otherwise did not sent out a response appropriately and as required. It is highly improbable that this would be the first case of such an occurrence.
>
> […]
>
> The following steps are taken by AHS prior to issuing disclosure packages to ensure that are sent to the correct parties, and not inadvertently sent out with other mail:

> • Confirm that the address on printed envelope/label matches the address on the corresponding response letter and compare to the access request provided by the applicant. Double-check before submitting to the Outgoing Mail.
>
> • Handle only one response package at a time (i.e. print response letter, print applicant's copy of records, and print mailing address on envelope/label all at once). Place printed response letter and records into envelope and seal. Immediately place envelope through postage machine and place in Outgoing Mail basket. The printer, postage machine, and Outgoing Mail basket are located immediately beside each other.
>
> • Only one access response is included in each disclosure package. Should an Applicant have multiple access requests, multiple disclosure packages will be issued.
>
> • Disclosure packages are limited to the response letter and the enclosed records. They are not to contain other correspondence of any kind.

[para 17] The Public Body has provided its reasons for believing that its Advisor placed the disclosure package in the outgoing mail area where an administrative assistant was expected to mail it out. The Public Body did not provide evidence as to why it believes the package was mailed out by an assistant or pinpoint a date on which the assistant sent out the package, but surmises that it was sent out on May 6, because that is the date of the cover letter, and because the Public Body's procedures indicate that the package should have been sent out on that day or the next day .There is no evidence that the package wasn't mailed out; however, the fact that the package did not reach its destination, despite being properly addressed, raises this possibility.

[para 18] The Complainant states:

> Why[is] there no "process" in place to actually record a date perhaps use of a date stamp when the actual document leaves the "out going basket" into the general mail instead of wondering as is in this case the documents were either sent on the Friday or Monday or for that matter later in the week?
>
> […]
>
> […] "the Advisor who completed the processing of this request had completed over 700 access requests over a sixteen (16) year career with AHS(and his predecessors). Not once has it been alleged that he forgot or otherwise did not send out a response appropriately and as required. It is highly improbable that this would be the first case of such an occurrence" We are all human beings and you can't tell me we "never make a mistake." […]

[para 19] I agree with the Complainant that it would be helpful if the Public Body had in place a process by which it could confirm when disclosure packages were mailed out. Many public bodies do document when disclosure packages are mailed out as this assists them to demonstrate that they have met the terms of section 11 of the FOIP Act when it is necessary to do so. In this case, it would provide a degree of comfort to the Complainant if the Public Body consulted its records and discovered that an administrative assistant did not mail out the package. Such a discovery would also negate the need for an inquiry.

[para 20] I accept that the Public Body's Advisor has processed over 700 access requests in a sixteen-year career. However, as the Advisor is not the person responsible for mailing packages, but administrative assistants are, according to the Public Body's evidence, the experience of the Advisor is not clearly determinative of the question of whether the Public Body mailed out the disclosure package.

[para 21] Regardless, the Public Body has conceded for the inquiry that it mailed out the package, and has established that it very likely correctly addressed the disclosure package, given that the cover letter was properly addressed and given the steps its employees take to ensure that mailing labels match cover letters. The Public Body has also submitted evidence that it has measures in place to ensure that disclosure packages are not inadvertently mixed with other correspondence or disclosure packages intended for others. I accept that the Public Body mailed out the package, given that it concedes it did.

[para 22] I note that correspondence and packages are not always received by the appropriate party even when they are sent by courier or a form of registered mail. I agree with the Public Body that the fact that a package was not received does not mean that it failed to take reasonable measures to mitigate the risk of unauthorized disclosure. I find that the Public Body's decision to send the package by regular mail was reasonable, given the *Workers' Compensation Board* decision and the steps the Public Body took to ensure that the package was appropriately created and addressed. However, I recommend that in future, the Public Body consider implementing a process by which the date a disclosure package is mailed and the initials of the person who mailed it are recorded, if it does not already have such a process. This would enable it to provide better evidence in relation to complaints of unauthorized disclosure or failure to meet statutory timelines.

[para 23] To summarize, I find that the Public Body took appropriate steps within the terms of section 38 to guard against the risk of unauthorized disclosure when it mailed the disclosure package on May 6, 2016.

III. ORDER

[para 24] I make this Order under section 72 of the Act.

[para 25] I confirm that the Public Body met its duties under section 38 of the FOIP Act when it mailed the disclosure package to her on May 6, 2016.

_____

Teresa Cunningham
Adjudicator
/ah