NORTHWEST TERRITORIES
INFORMATION AND PRIVACY COMMISSIONER
Review Report 20 -244
Citation: 2020 NTIPC 48

File:19-263-4
September 29, 2020

Compliance Issue: prevention of unauthorised use and disclosure, protection of information, collection of information

Key Words: accuracy, limited disclosure, privacy safeguards, breach response NTHSSA, ECE, privacy breach response plan, staff training and awareness

Public Body: Education, Culture and Employment

BACKGROUND

This matter relates to a record containing personal health information (PHI) that was received by the Department of Education, Culture and Employment (ECE) from an NWT health clinic in July 2019. The PHI that is the subject of this review pertains to two unrelated patients referred to in this review as "Patient A" and "Patient B". The record in question was a "Form D - Disability Assessment (Form-D)" used by ECE in determining an individual's eligibility for income benefits.

As background, Patient A and Patient B had attended separate appointments at the Frame Lake Community Health Clinic (FLCHC) in Yellowknife on the 9th of July, 2019. Patient A sought a medical certificate (Form-D) which is used by ECE to determine if an individual qualifies for disability income assistance. Patient B sought a Driver's Medical Assessment required by the Department of Transportation (DOT) for road licensing.

Both forms used in the medical appointments, the Form-D and the Driver's Medical Report, have dedicated space on the top of the first page for the patient or physician to write the patient's name, date of birth, and contact information. There is also a space for

the patient to sign and date the form that documents their express consent to collect this information for purposes identified at the time of the collection. The remainder of the Form-D contains a number of questions intended to document the personal affairs and the medical conditions of the patient. When completed, the Form-D contains extremely sensitive personal information about the mental and physical health of the individual.

In this case both patients signed and dated their respective forms, giving consent to collect, use and disclose their information, in the case of Patient A to ECE regarding income assistance, and in the case of Patient B to DOT to qualify for road licensing. Patient B filled in the top portion of the Driver's Medical Form but the evidence before me suggests Patient A or Patient A's physician did not fill in some or all of the top portion of the Form-D or, if filled in by hand, the section was not entirely legible.

Patient A's physician apparently asked the nurse who had assisted with the appointment to add a label to the top portion of the form - this being a printed address label containing standard patient identifiers including: full name, address, telephone number, date of birth, health care number of the patient, as well as physician name. The nurse generated a label using information stored in the territorial electronic medical record (EMR) and applied it to the top portion of the Form-D overtop of the name and address section. Unfortunately, however, the nurse attached the wrong label - she affixed a label containing Patient B's identifiers to the Form-D instead of Patient A's. The two page Form-D was then faxed to the ECE Service Centre.

On July 9th, 2019 ECE received the fax from the FLCHC. On that day an ECE Administrative Assistant put the fax into a Client Services Officer's (CSO) office mail box for processing. On the 12th of July, the CSO determined that the individual identified on the Form-D was not their client and faxed the entire form back to FLCHC, and then securely discarded the hard copy.

The clinic is managed by the Northwest Territories Health and Social Services Authority (NTHSSA). NTHSSA became aware of the breach on the 12th of July when FLCHC staff retrieved the fax from their fax machine and read the note on the fax cover sheet sent by ECE that read: "To: [name variation] - Frame Lake … "Form D-Disability WRONG applicant information…". The note on the fax is how the Authority discovered the breach.

After the Chief Operating Officer responsible for FLCHC notified my office about the breach in August 2019 I initiated a formal review of FLCHC's handling of the information, under NTIPC file #19-213-6. During my investigation, I approached ECE for information about related handling of the information. I questioned why the CSO did not simply phone the clinic to report the breach, as instructed on FLCHC's fax cover sheet, instead of re-faxing the entire form. I inquired with ECE about staff training in privacy and if they had a breach response plan. ECE could not confirm if any of the ECE staff had completed what was described as "required" training in ATIPP (access to information and protection of privacy) as part of professional development. Further, although some 'security' protocols were in place, ECE did not have privacy breach response plans as a measure to ensure information was protected from further use and disclosure.

While apparently infrequent, based on the facts of the matter, I expect similar breaches are not unlikely and it is therefore important to ensure an appropriate response from ECE. Given the apparent lack of safeguards in place to ensure personal information was protected when responding to a privacy breach I determined that the matter warranted review.

I would like to note that ECE was highly assistive in response to my review of the matter, providing documentation and fulsome responses to my inquiries about its business processes as they relate to breach response and processing a Form-D.

THE RECORD

This Form-D was developed by ECE to document a medical assessment or "medical certificate", referred to specifically under section 21 of the *Income Assistance Regulations*, as: "…a medical certificate setting out the condition of health of an applicant as an aid in determining the applicant's employability or ability to participate in an activity or program…". This information received by ECE from the medical practitioner is highly "confidential" per section 12.1(2) of the *Social Assistance Act* (SA Act).

Under the SA Act, the CSO may require an individual to provide a completed certificate to determine qualification for one or more allowances related to a disability allowance managed by ECE's Income Assistance Program. Per ECE's "Income Assistance Policy Manual", the Form-D must be completed by a licensed practitioner and "must be faxed directly from a health care professional's office". ECE states that the completed form cannot be accepted directly from an applicant as a measure to ensure the integrity of the information provided on the form.

In addition to the personal identifiers - these being full name, mailing address, telephone number, DOB, and community name - the Form-D also records a brief description of physical and mental impairments and abilities, various medical conditions, relevant past injuries, addictions and chronic diseases. The form documents if, in the opinion of the medial practitioner, the impairment suffered by the client was "permanent", "recurrent", "long term" or "short term", and collects the practitioner's statements relating to the capacity of the applicant to manage their own affairs and self-care. In all, the information is highly personal and extremely sensitive in nature.

There are no instructions on the form as to how it is to be completed or by whom save for a note clearly directed to the medical practitioner explaining what ECE uses the medical opinion for and the criteria to be met for a disability allowance. Nowhere on the

form does it state that the form is "confidential" when completed, though it does state on the bottom that "the privacy provisions of the ATIPP Act protect information…".

ISSUES

As public bodies, each with duties to the public to protect personal information and prevent its unauthorized use, including in this case to control a breach and correct inaccurate information, both NTHSSA and ECE shared responsibility in responding to the breach, but as ECE is the organization that discovered the breach, there was significant reliance on measures ECE had in place at the time to respond appropriately to the error. As well, there was also a reasonable requirement for ECE to respond according to measures FLCHC had put in place to address the receipt of information in error.

In reviewing both NTHSSA's and ECE's response to the situation, I gained a sense that the actions taken by the CSO at ECE in this case were not appropriately measured. I further suspected the CSO's actions reflected more a lack of awareness of existing governance and of best practices than any intent to respond without necessary regard.

The issue to be determined is if ECE responded to the discovery of the error appropriately, if the CSO handled the personal information in accordance with requirements under applicable legislation and if there are sufficient safeguards in place to prevent further unauthorized use and disclosure of personal health information. I also reflected on risks with respect to information sharing in the context of these two organizations.

The following key issues form part of this review:

1. Do the *Health Information Act* (HIA) and/or the *Access to Information and Protection of Privacy Act* (ATIPPA) apply and do I have jurisdiction?
2. Did ECE have authority to collect, use and disclose the information?
3. Did ECE have adequate measures in place to respond to a breach?
4. Did ECE respond appropriately to the breach?

1. Does HIA and/or ATIPP apply and do I have jurisdiction?

A completed Form-D is used by ECE to determine if an individual qualifies for one or more benefits managed under the authority of the *Social Assistance Act*, and *Income Assistance Regulations*. The SA Act and regulations make no mention of ATIPPA or HIA. I needed to determine if either or both might apply in this case.

ATIPPA applies "to all records in the custody or under the control of a public body" pursuant to section 3(1) of the Act. It is necessary then to determine the following:

a) if ECE is a "public body",
b) if the information "personal information" as defined under ATIPPA, and
c) if the information in this case was in the "custody or under the control" of ECE.

<u>Public Body and Personal Information</u>

A "public body" pursuant to section 2 of ATIPPA includes: "(a) a department, branch or office of the Government of the Northwest Territories,…".

Under section 2 of ATIPPA "personal information" is defined as:

> s.2. "personal information" means information about an identifiable individual, including
>
> (a) the individual's name, home or business address or home or business telephone number, …

(d) an identifying number, symbol or other particular assigned to the individual, …

(f) information about the individual's health and health care history, including information about a physical or mental disability, …

I find that ECE is a public body, and that the information of both Patient A and Patient B recorded into the Form-D is "personal information" as defined under the ATIPP Act.

Custody or Control

The record in question was received by and intended to be used by the ECE office to determine if a client qualified for income assistance. Under ATIPPA employees are charged with a duty to appropriately handle personal information, and pursuant to section 47.1 of ATIPPA "shall not, without authorization, disclose any personal information received by the employee in the performance of services for a public body".

I find that the CSO is an employee of a public body who received this information in the performance of a service for the public body, and thus ECE had custody of the record in question at the time the breach was discovered.

Application of Legislation

I find that three Acts are applicable to this review - ATIPPA, HIA and the SA Act. There do not appear to be any conflict or inconsistencies in their application. ATIPPA is foundational and dictates appropriate responses.

2. Did ECE have authority to collect, use and disclose the information?

Collection

Section 40(a) of ATIPPA requires that personal information collected relate **directly to**

and be **necessary for** an existing program or activity of the public body.

> 40. No personal information may be collected by or for a public body unless
>
> (a) the collection of the information is expressly authorized by an enactment;
>
> (b) the information is collected for the purposes of law enforcement; or
>
> (c) the information relates directly to and is necessary for
>
> (i) an existing program or activity of the public body, or
>
> …

The disability income assistance program is such a "program" pursuant to subparagraph 40(c)(i). When correctly completed and subject to the *Income Assistance Regulations* s. 21, the Form-D information directly relates to and is necessary for an individual to participate in that program:

> 21. An Officer may, at any time the Officer considers it necessary, require a medical certificate setting out the condition of health of an applicant as an aid in determining the applicant's employability or ability to participate in an activity or program referred to subsection 13.1(6).

Further, the Form-D disclaimer on the bottom of the first page claims authority for ECE to collect the information under ATIPP s. 41(1)(g). Section 41(1)(g) of ATIPP states:

> 41.(1) A public body must, where reasonably possible, collect personal information directly from the individual the information relates to unless

g) the information

(i) is necessary in order to determine the eligibility of an individual to participate in a program of or receive a benefit, product or service from the Government of the Northwest Territories or a public body and is collected in the course of processing an application made by or on behalf of the individual the information is about, or

(ii) is necessary in order to verify the eligibility of an individual who is participating in a program of or receiving a benefit, product or service from the Government of the Northwest Territories or a public body and is collected for that purpose;

I find that the Form-D or "medical certificate" information is necessary information supporting a determination as to the eligibility of an individual to receive a benefit from the GNWT's income assistance program, and ECE is authorized to collect the information under ATIPPA s. 40, and 41 supporting s. 21 of the *Income Assistance Regulations.*

Collection - Personal Health Number (PHN)

Though it is entirely reasonable for ECE to collect the completed Form-D in support of an individual's application to the Income Assistance Program, in this case FLCHC disclosed the wrong information. FLCHC also disclosed more information than was necessary for ECE's purposes - a blank FORM-D does not include fields to collect a patient's personal health care number (PHN). This indicates that ECE does not need this information for its purposes. However, the label applied by FLCHC additionally disclosed the patient's PHN.

While these are contraventions, I find that ECE did not knowingly contravene the Act with respect to collecting Patient B's as opposed to Patient A's information, as this circumstance is not of ECE's making. Given protocols with respect to the application of labels regularly followed by FLCHC, it is reasonable to believe that ECE regularly receives Form-Ds completed with a label affixed to the top portion of the form, and that ECE has been collecting the PHN of clients over time without a clearly identified need with respect to the income assistance program. Further, the HIA is prescriptive as to the collection of a patient's PHN. It can only be collected or used for specific purposes under s. 32 of HIA which provides that:

> 32.(1) A person other than an individual who is assigned a personal health number or a health information custodian, shall not collect or use the individual's personal health number unless the collection or use is required
>
> (a) for a purpose for which a custodian has disclosed the number to the person;
>
> (b) for a purpose permitted by an enactment or by an Act or regulation of Canada; or
>
> (c) for a prescribed purpose

I find that ECE unwittingly collected too much information from FLCHC, notwithstanding that ECE's did not request the PHN on its Form-D. Assuming that this is not a "one-time" event, ECE has most likely collected PHNs in this manner in the past. This should be addressed.

Collection - Valid Consent

An individual's permission or "consent" is generally required when a public body collects that person's personal information, though there is nothing in the ATIPPA which requires that consent for collection purposes. Without the express consent of the

individual, however, ECE would be unable to collect the necessary information. Without going into the rather complex details of consent to collection of personal health information under HIA, barring limited exceptions that do not apply in this case, FLCHC requires the consent of the individual in order to disclose the individual's personal health information through the Form-D.

The Form-D clearly requests and documents the consent of the individual by way of the following statement: "I hereby release the following information to the Department of Education, Culture and Employment Government of the Northwest Territories". The date and signature fields that follow the statement clearly are intended to document the individual's express consent to this disclosure of information to ECE.

Consent to the collection is also required under HIA. Without going into the rather complex details of consent to collection of personal health information under HIA, and barring limited exceptions that do not apply in this case, FLCHC also requires the consent of the individual before it can disclose the individual's personal health information through the Form-D.

In this case, Patient A clearly signed and dated the form giving permission for what one would expect to be an accurate and complete description of their person specific identifiers, medical conditions, and related information and professional medical opinions, and for this to be transferred to ECE in the completed Form-D. Without this valid consent, the information cannot be collected or the form released to ECE by FLCHC.

In this case, the written consent was of Patient A, not of the individual identified on the top of the form - Patient B. Further, it is doubtful Patient A's consent is valid after the nurse applied the wrong patient identifiers to the form. The error put NTHSSA in a position of unauthorized disclosure of both patients' information and put ECE in the

unintended position of collecting information ECE was not authorized to have without valid consent.

Use

The ECE "CSO Resource and Procedure Manual" states "the CSO can only use the information collected for determining the applicant's initial and continuing eligibility" for assistance. Also, section 43 of ATIPPA states that a public body may "only" be used as follows:

> 43. A public body may use personal information only
>
> (a) for the purpose for which the information was collected or compiled, or for a use consistent with that purpose;
>
> (b) if the individual the information is about has identified the information and consented, in the prescribed manner, to the use; or
>
> (c) for a purpose for which the information may be disclosed to that public body under Division C of this Part.

ECE requires the completed Form-D or "medical certificate" to aid in making a determination as to the eligibility of an individual to receive a benefit from the GNWT's income assistance program. With respect to s. 43, ECE is authorized to use the information, for the purpose it was collected subject to s. 5 of the regulations. Subsection 5 (a) and (b) are as follows:

> 5. The consent of an individual to a public body's use or disclosure of his or her personal information under paragraphs 23(4)(a), 43(b) and 48(b) of the Act
>
> (a) must be in writing; and
>
> (b) must specify to whom the personal information may be disclosed or how the personal information may be used.

The Form-D "Consent" section identifies ECE as the entity that the information will be disclosed to. In my opinion, the form is too broadly worded. It should not identify the entire Department of ECE as the authorized recipient, but the Income Assistance Program. However, with respect to the use of the information, the Form D meets the minimum requirements of section 43 of the Act and 5 of the regulations specifying to whom the information may be disclosed.

Use - Accuracy

Before it can use the information, ECE must ensure the information is accurate and complete per section 44 of ATIPP. Under s. 44 the duties of a public body include:

> 44. Where a public body uses an individual's personal information to make a decision that directly affects the individual, the public body must
>
> (a) make every reasonable effort to ensure that the information is accurate and complete; ...

The information transmitted to ECE was not accurate - it included the wrong patient's personal identifiers and contained additional information ECE did not require to process the application for income assistance. The CSO determined upon receipt that the information was inaccurate. They did not proceed with use of the information for the purposes the information was collected. To do so would not only have contravened s.44, it would have been unreasonable given the circumstances.

I find that in the circumstances, that the CSO took appropriate steps to ensure the accuracy and completeness of the information in making the determination not to use the information.

I find that ECE was compliant with its use of the information under s. 43, 44 of ATIPPA and s. 5 of the regulations.

Disclosure

Section 48 of ATIPPA states that ECE may disclose personal information:

> 48. A public body may disclose personal information
>
> (a) for the purpose for which the information was collected or compiled or for a use consistent with that purpose;
>
> (b) where the individual the information relates to has identified the information and consented, in the prescribed manner, to its disclosure;
>
> …

While the SA Act is silent on collection and use, the SA Act is prescriptive with regards to disclosure of the same information. In this case, pursuant to s. 12.1(1)(a) of the SA Act, other than in respect of forgiveness of a debt or exchange of information in respect of a benefit already paid, the information collected under the SA Act can only be disclosed with the consent in writing of the person the information relates to.

In addition to ATIPPA and the SA Act, as a further requirement to disclosure of that same information HIA s. 39 also applies. Under s. 39 of the *Health Information Act* ECE is deemed to be a "recipient" of that information, and as a "recipient", ECE is held to s.40(3) of HIA which provides that a recipient, being not a custodian or person the information is about, "shall not disclose more information that is necessary to meet the purpose of the use or disclosure".

Thus, to disclose the information further ECE would be required to

1) have the individual’s express consent,

2) not disclose more information than necessary to meet the purpose of the use or disclosure,
3) must only use the information for the purposes for which the information was collected or for a use consistent with that purpose, and
4) can disclose information only if the individual that has given their consent to the disclosure.

In this case, the CSO determined the Form-D information was wrong and did not further disclose the information except in regards to notifying NTHSSA of the error by sending it back to the FLFHC by fax. This latter action does not align with the above provisions under ATIPPA for disclosure. I will deal with the matter of faxing the entire form back in section 4 of this review.

3. Did ECE have adequate measures in place to respond to a breach?

The purpose of the ATIPPA includes to make public bodies more accountable to the public and to protect personal privacy. This includes, in section 1(d), "preventing the unauthorized collection, use or disclosure of personal information by public bodies". Further section 42 requires that: "the head of a public body shall protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.". Part of ensuring information is protected and remains secure is having measures in place to immediately respond when personal information is at risk and to ensure information is protected from additional contraventions of the Act when a breach occurs.

<u>Privacy Breach Plan</u>

ATIPPA is not particularly helpful in directing responses to a privacy breach, but most public bodies have guidelines or formal processes in place to guide employee's responses to breach incidents. The GNWT does provide high level guidance in this

regard. As such, most employees are subject to minimum reporting and initial breach response requirements.

While ECE did not have responsibility for what was in the received record, it did have custody of the record and thus was responsible to ensure appropriate handling of the information it received from FLCHC. It was necessary for ECE to respond to the breach once discovered even though it was not the author of the error. Though ECE did notify the responsible organization, there were issues with that response.

I requested information from ECE about their privacy breach policy, procedures or guidelines in place that might reflect the CSO's actions in this case. ECE provided a fulsome response to my office's inquiry, including providing several reference documents. ECE provided the "GNWT Access and Privacy Office, Department of Justice, Breach Notification Tool" which states: "If a breach occurs… the breach should be reported to the public body that has primary responsibility for the personal information". This protocol also states "Do not share personal information with these other entities unless required". Though this advice is directed at offices like mine, it at least recognizes the importance of limited disclosure.

Unfortunately the notification tool provides little direction on initial response to a privacy breach, except for reporting it to the "responsible" organization. The tool is clearly intended to be used more as an aid in determining if a client should be notified about a breach or not, and is not, therefore, entirely applicable in this case. As it was, FLCHC notified the affected individuals about the breach.

ECE also provided me with "Information Security Incident Reporting" guidance issued by the GNWT. This too misses the mark with respect to responding specifically to a "privacy" breach, as opposed to a "security" breach.

ECE additionally provided a copy of "Conducting a Privacy Complaint Investigation", also developed by the DOJ. The document is "complaint" specific – that is, it is focused on an individual making a complaint about the government's handling of their own personal information. Other than a reference to "destroying or returning information that was inappropriately collected" and recording information about the incident, this document is not well suited to guide any employee in their initial response to the breach of a third party's privacy, which needs to include controlling, reporting and responding while ensuring limited additional disclosure and optimal protection of that information.

These references do not provide clear guidance to an employee as to key steps they should take in such circumstances - the nuts and bolts of breach response when they first discover a privacy-specific breach. The steps I would expect to see in such guidance might include but not be limited to:

- prevent further unauthorized use and disclosure by retaining the record in a privacy protective and secure manner;
- immediately report the breach to your supervisor without sharing personal information;
- report the breach to the responsible organization without sharing personal information;
- in cooperation with the responsible organization determine the information needed to clarify the breach and record in question - share only this information;
- if the responsible organization requests the record be returned, use the most secure and privacy protective means available to transfer the record (avoid using fax if a more privacy protective means of transmission is feasible);
- if the responsible organization requests the record be destroyed, use the most appropriate means to destroy the record, and confirm the destruction with the organization after the record has been securely destroyed;

- keep a record of the nature of the incident and relevant details without recording personal information

Staff Training

When I asked about the document security or privacy training completed by ECE staff, ECE responded that there is mention of confidentiality in the Client Services Officer Resources and Procedures Manual, and that staff are taught about confidentiality of records 'on the job'. ECE offered that "All staff are required to take ATIPP Act training, as part of their professional development", however, ECE also admitted that "the Service Centre cannot confirm that the North Slave staff have taken this training, or document security training".

I determined that ECE does not have a comprehensive privacy breach response plan, does not have practical guidance in place that staff can easily refer to should they discover the type of errors found in this case, and has not ensured that all staff who handle sensitive personal information have been trained in privacy and privacy breach response.

I find that ECE did not have measures in place sufficient to respond to a privacy breach, and therefore lacked means to protect information in its custody or under its control, as intended and required by the ATIPP Act.

4. Did ECE respond appropriately to the breach?

Troubleshooting - Not Business as Usual

The applicable sections of the ATIPPA, the SA Act, and HIA direct the normal course of business when handling personal information. In this case, the intended business context was to collect the information and evaluate an individual's qualification for

income support. ECE is held to this purpose when contemplating use and disclosure of that information. In this case, however, the normal course of business was interrupted.

Unfortunately, the current iteration of ATIPPA is not particularly helpful in framing how information should be handled in such circumstances - the Act lacks the expected privacy breach provisions found in similar legislation such as the *Health Information Act*.

However, privacy principles do not change just because the normal course of business is disrupted, and these principles can be applied to troubleshoot situations when information is received in error, just as they are used in day to day handling of personal information. Thus, the same basic principles that are foundational to ATIPPA and to privacy and privacy best practices, continue to apply in responding to a breach and with respect to disclosures related to the error. This includes, generally, to only disclose information for a needed and reasonable purpose specific to the circumstances while ensuring that only those needing to know the information are privy to it.

Further, though not explicit in such circumstances, the current version of ATIPPA directs that the response reflect the spirit of the Act. Pursuant to 1(d) the purposes of the Act include to make public bodies more accountable to the public and to protect personal privacy by preventing the unauthorized collection, use or disclosure of personal information by public bodies.

In short the information can only be handled as reasonable and necessary to meet the needs of the original intended collection of that information and to address related risks to the security and privacy of that information. With this in mind, the CSO needed to control the situation, and both alert the responsible organization of the error and, as a measure reflective of the original purpose of collection, take steps to gain the correct information so they could process Patient A's request.

Limited and Purpose Specific

The next question, then, is what information needed to be used or disclosed in this case in order to troubleshoot this situation and in order to meet the original purpose of the collection? Did ECE honor basic privacy principles in sending the entire two-page Form-D as an adjunct to reporting the error? The fact the record was faxed back to FLCHC in the absence of a request that they do so is a bit concerning. Could the necessary step of reporting the error and gaining the correct information not have been achieved without transmitting it and yet again disclosing the entire record to someone who does not necessarily need to know the personal information?

In my opinion, a reasonably measured approach was not taken by ECE in handling of the record after the error was discovered. The CSO could have easily reported the error without disclosing the entire record. If necessary, the CSO may have used or disclosed part of the record to resolve the matter and ultimately achieve the purpose the information was intended for in the first place. This might be permissible under 43(a) and 48(a). More specifically, some of the information could be used or disclosed "consistent with" the purpose for which the information was collected, which in this case was ultimately to process Patient A's application for income assistance. In this case, since FLCHC was the author of the record, it clearly had a copy of it and re-transmitting the record was, therefore, unnecessary.

It is not always necessary that the breached information be re-transmitted as a means to report a breach. A breach can and should be reported initially without sharing any personal information. What should be shared after reporting the breach follows the same principles used where it is business as usual, including: disclose only as necessary, with reasonable and specific purpose to the original collection and in the circumstances, and all the while protecting the information from unauthorized access, collection, use and disclosure.

I find that because ECE received the information in error and was required to gain the correct information, it was as necessary reasonable to make a limited disclosure of the personal information, but that it was not necessary to disclose the entire record for this purpose.

Adherence to Safeguards

As stated, there is no specific provision under the current version of the ATIPPA that requires a public body to respond in a prescribed manner in the event of a privacy breach, either one caused by the public body or in responding to a breach caused by another organization. What ECE had in place at the time to manage such an indecent was lacking, and not particularly helpful to front line staff having to stick-handle such an incident.

Despite this lack of direction, and though things could have been done differently, it should be acknowledge that the CSO's response was mostly in accordance with best practice and more or less followed the fragmented guidance referenced above. The CSO:

- verified the accuracy of the information when received
- did not use the information to make a decision about the individual
- controlled the document to prevent additional unauthorized use
- did notify FLCHC of the breach as soon as they identified it
- used a fax cover sheet to protect the information they forwarded to NTHSSA
- securely destroyed the record per the instructions that appear at the bottom of NTHSSA's fax cover sheet which reads: "If you have received this communication in error please destroy it".

That said, some of the actions taken by the CSO were not in line with ATIPPA, HIA, and privacy best practices, and as a result the already breached information was subjected to additional risk, and too much information was used and disclosed for the purposes of

reporting the breach. The CSO also did not report the breach to their own manager, so management could not make a determination if the error was an issue they needed to follow up on. The CSO also did not follow the instruction on NTHSSA's fax cover sheet that very clearly directs the receiver to report by phone if an error is detected.

ECE did not report the breach by phone before returning the record to NTHSSA. ECE did not verify what information NTHSSA needed for their investigation, before disclosing personal information back to FLCHC and destroying the evidence. Rather, the CSO sent a fax to the FLCHC fax number addressed to someone identified by what appears to be a name variation of their first name (purely an example - "Bettie"). If the fax had been misdirected, a very real possibility, another disclosure could have easily occurred in the act of faxing it back to FLCHS.

Given the lack of governance at ECE for breach reporting, I cannot fail the CSO for responding in the manner that they did. There was little clear or coherent guidance to adhere to. I conclude the CSO's response was based primarily on their own sense of how they should address the situation. This resolved the matter but put the personal information at addition risk. This reflects ECE not having a dedicated privacy breach response plan in place and inconsistent training provided for its employees.

I also note that the instructions provided by NTHSSA to safeguard personal information when received in error were not abided by. These instructions, written on the bottom of FLCHC fax cover sheet were only partially followed, causing the CSO to use the fax instead of phoning to report the breach.

FLCHC is reliant on ECE to appropriately report errors in a manner that mitigates risk, and abides by measures FLCHC has put into place to protect this information. Phoning to report when personal information is disclosed in error is a measure implemented

pursuant to subsection 13(j) of the HIA: "procedures that provide for effective prevention of, response to and remediation of security and privacy breaches."

I find that ECE failed the CSO by not ensuring the employee had resources and training that would impart the skills and knowledge required to respond appropriately to a privacy breach and limit the disclosure of any personal information that had already been breached.

DISCUSSION

Ideally the person who discovered the breach would report it to their supervisor, secure the record in question, report the breach by phone to the other organization's designated contact person, and take direction from the responsible body as to the level of detail required for their purposes in addressing the record in question.

This detail may not include sharing personal information, or may require some or the entire record be handed over as evidence to support the responsible organization's investigation and to correct the information. The responsible organization may ask that the information be transferred to them securely, or destroyed in a secure manner.

What should be done with the record once the breach is reported? This is another matter that should be discussed with the responsible organization. I have to say in this, I do not agree with the instructions NTHSSA has on the bottom of their form which is to immediately destroy the record. The record should ideally be secured by the receiver, the breach reported, and the receiving organization should not destroy the record until the responsible organization has indicated what they want done with the record. Often the record is needed as evidence to assist with the investigation, and to understanding what happened, and how the breach should be responded to. The responsible

organization may also need that information to identify the individual whose information was breached in order to notify the individual of the breach.

Limited Disclosure

There is good reason to phone in a breach, as opposed to sending a fax and hoping it gets to someone who can respond to the error. NTHSSA became aware of the breach only after the fax was retrieved from the fax machine by staff at FLCHC.

Phoning to report a breach is an important step that permits identifying the correct person to report the breach to, allows for reporting without disclosing personal information, and permits verification of what information may need to be disclosed to clarify the breach before disclosing it. It also gives the responsible organization an opportunity to advise on the most appropriate means to handle the information on the receiver's end. Phoning may also be more timely as a means of breach notification, as opposed to relying on someone eventually noticing a note written on a fax sitting on a fax machine.

Another very good reason to phone is to prevent yet another privacy breach. More often than I would like to report, employees treat a record involved in a privacy breach like a "hot potato". By email or fax or other means of communication, the breach and the records get passed on down the line, and the breach repeats until it lands in the hands of someone who is aware of how to deal with a privacy breach. By that time, many people with no operational need to have access to the personal information have handled the document.

Faxing and not phoning risks subjecting the information to yet another error, either a technical error or human error, possibly transferring the record to the wrong recipient, or even the wrong organization. There have been many instances of a breach of privacy caused by a fax being misdirected. The initial error could have caused a much larger

breach if the fax sent by the CSO had been inadvertently sent to the wrong recipient. In the wrong hands Patient A's medical prognosis might be attributed to Patient B. In this case the additional risk was unnecessary as there was no need to transfer the record back to FLCHC as the clinic had a copy on file.

Lastly, this is a situation where "more is **not** better". An internationally recognized privacy principle requires limited disclosure of information as needed. Again, given NTHSSA's records practices the CSO did not actually need to send the entire Form-D back to FLCHC. Phoning ahead could have clarified the matter.

Shared Safeguards & Integrated Service

I'm concerned that the CSO ignored the direction on FLCHC's fax cover sheet, as this measure is a safeguard that FLCHC has implemented pursuant to section 13 of the HIA regulations to protect information. It is important that ECE respect the efforts of other public bodies to protect personal information.

Furthermore, the record in question is reflective of an integrated service - ECE's income support program and NTHSSA's primary health care services, with each public body being duty bound to the other to appropriately handle the information. Unfortunately in this case, each failed the other and failed the individuals whose information was not handled well.

I was not advised that there is an agreement or other formalized understanding between ECE and NTHSSA to address the rather important information management aspects of the requirements of the Income Assistance Program. ECE is dependent on NTHSSA to collect information about patients, and ensure the accuracy of that information when it is disclosed to ECE. NTHSSA is relying on ECE to only use or disclose the information as lawfully permitted, including to advise of errors in the most secure and privacy protective way possible.

Not just ECE, but all public bodies should be cognizant of the efforts other organizations have put in place to best manage the personal information they collect, use and disclose. Such an approach aids in managing risks and both respects and protects privacy of the individual(s) the information relates to. This is sensitive personal information, often of a shared client, and who is reliant on more than one organization to do the right thing and handle their information appropriately, regardless of the nuances of this or that legislation.

Final Word

Some key issues were identified in this review, but it was focused on a very narrow fact situation. It did, however, raise more general concerns as to ECE's approach to handling of all types of information. I would encourage ECE to catalogue the types of information it receives and identify options to ensure that privacy protective means are used to receive and transmit sensitive personal information. ECE did indicate in its response to my office that the Department is considering alternate solutions to securely transfer information between health clinics and ECE going forward. I also would encourage ECE to invest in a dedicated breach response plan and ensure ECE employees are well prepared through training and awareness, to address privacy specific incidents.

CONCLUSION

Government departments and health regions do not work in a vacuum. Collection and sharing of information between government agencies is often necessary in order for the government to provide the public with the services they need. This case highlighted the interdependence of organizations and reliance on the others to handle information in a certain way.

Organizations have to do more than simply rely on the lawful obligations of the organizations they do business with to meet legislated requirements to handle information appropriately. Policy, procedures and staff awareness and training are key to ensuring appropriate handling of client's most sensitive information at all times.

In addition, where programs are integrated and sensitive information will be disclosed, dialogue between the two organizations is critical. There needs to be clear, relatable agreement as to how each organization will meet its responsibility to the other and to the public. It should be clear how they will each appropriately handle sensitive information, including to ensure accuracy, completeness, and limited disclosure, and to address breach incidents in a timely and privacy protective manner.

Each must have policy, procedures and appropriate training programs in place and ensure administrative tools in place and applied to effectively manage related risk. To do otherwise is contrary to the provisions of not just legislation, but privacy best practices and the trust individuals place in our public institutions.

RECOMMENDATIONS

Pending amendments to the *Access to Information and Protection of Privacy Act,* which were passed in the last Legislative Assembly and are awaiting a “coming into force date”, will impose significant additional responsibilities on public bodies to protect personal information and to report and respond to privacy breaches. This review was an opportunity to bring gaps and issues of privacy governance into focus. Plugging such gaps now will better align ECE with current requirements and will put ECE in a better position to meet their responsibilities when the amendments come into effect.

1. I recommend that ECE add directions to its Form-D that instructs patients and physicians that the top portion of the form is to be completed by the patient (or

the physician). I suggest the instructions ask for at least two pieces of identifying information (e.g. name, DOB);

2. I recommend that ECE take steps to prevent collection of personal information into the Form-D that is not needed by ECE to determine the applicant's initial and continuing eligibility for income assistance services (e.g only collect PHN if authorized under HIA and if require by ECE for the reasonable and identified purposes consented to). I would encourage ECE to review its records and remove (redact) any PHNs which they have inadvertently collected in error.

3. I recommend ECE ensure all of its staff have been trained in privacy best practices and are aware of generally accepted fair information principles;

4. I recommend ECE ensure all of its staff who work with personal information and/or personal health information have been trained in privacy specific breach response and are aware of where to find the breach plan for ease of reference;

5. I recommend ECE develop and institute a privacy specific breach response plan;

6. I recommend that ECE develop and institute a practical check list for staff to follow when responding to a breach that includes the following key measures:
    a. report the breach (not the personal information) internally to a designated person;
    b. retain the record in a secure manner for a reasonable time period until the responsible organization has an opportunity to provided direction as to the appropriate treatment of the record (this may include shredding or providing it to the originating organization in a secure manner);
    c. report the breach occurrence to the responsible organization initially without sharing personal information;

d. in cooperation with the responsible organization, determine the information necessary to share in order to clarify the nature of the record in question;
e. if the original or a copy of the record is requested to be disclosed to the responsible organization, use the most secure and privacy protective means available to transfer the record;

7. I recommend ECE keep a record of breach incidents that includes sufficient details to understand the nature of the breach, when it occurred, actions taken by ECE to address the incident and treat the record;

8. I recommend ECE explore more privacy protective options for receiving and transmitting sensitive personal information with respect to the Form-D.

In addition to these recommendations, I suggest that ECE and NTHSSA enter into a clear, relatable agreement as to how each organization will meet responsibilities to appropriately handle sensitive information shared between them, including to ensure accuracy, completeness, and limited disclosure, and to address errors and incidents in a timely manner. I suggest ECE initiate dialogue with counterparts at NTHSSA to identify and implement measures to:

- ensure accuracy and completeness of information disclosed to ECE (e.g. adding directions on ECE's form to encourage completion of the top portion prior to completing the medical portion of the form);
- explore secure means to transfer information (e.g. via encrypted electronic messaging);
- agree to respond to errors in a more privacy protective manner (e.g by phone, and by limiting information sharing to that which is necessary to report a breach);

- identify a contact person in each organization to notify if a privacy breach occurs (e.g designated contact person);
- Agree on parameters for when and how breached information should be destroyed.

Elaine Keenan Bengts
Information and Privacy Commissioner