NORTHWEST TERRITORIES INFORMATION AND PRIVACY COMMISSIONER
Review Report 20-HIA 26
Citation: 2020 NTIPC 23

Review File 19-165-06
April 21, 2020

BACKGROUND

On May 16th, 2019 my office received notice from the Northwest Territories Health and Social Services Authority - Yellowknife Region (NTHSSA-YK, or YK Region) of a breach of privacy discovered by the Authority on October 1, 2018. The breach was caused when a staff member working for the YK-Region faxed an individual's personal health information, intended to be received by the Worker's Safety and Compensation Commission, to the Motor Vehicles Branch of the Department of Transportation (DMV). The information transmitted included an individual's name, address, telephone number and a medical progress report including a description of the functional abilities of the individual and a statement made by a medical practitioner that the individual was currently not able to work.

The Authority reported the breach "was significantly influenced at the time by a high workload". The employee was in a rush and failed to clear the last number they had transmitted information to by fax before sending the next document. The WSCC fax number may or may not have been an "auto dial" number preprogramed into the fax machine, but the DMV number was preprogrammed and was reused in error in this case.

Once advised of the error the Authority reports that it retrieved the information, and at some point notified the affected individual. Management also reviewed the "faxing protocols" with the staff member involved, and did the same at a scheduled meeting with "all clinic staff".

Neither the breach notice received from the NTHSSA nor the Authority's response to my investigation identified the date on which the breach occurred or provided an adequate explanation as to why there has been more than six months' delay in reporting the breach to my office. After many attempts to clarify the nature of the breach with the authority in May, June and July of 2019, I finally received a response on the 8th of August. As this response was insufficient to clarify the nature of the breach and breach response, I requested clarifications, but did not receive a response to this letter.

APPLICATION OF *THE HEALTH INFORMATION ACT* AND OTHER LEGISLATION

The sections of the *Health Information Act* (HIA) engaged in this case pertain largely to the protection of personal health information, as well as the breach response by the custodian. The primary sections of the Act that are engaged include section 85 (protection of personal health information), s. 87 (notice of breach), and s. 13 and 14 of the regulations (safeguards/response). Also relevant is the Privacy Breach Policy created under the *Health Information Act.*

ISSUES

The Authority's response to the breach is the focal point of my concern in this case, as are the safeguards that should have been in place and been followed to prevent the breach. The timeliness of notification to the affected individual, and a lack of response to my office, are also discussed. This latter issue is an ongoing concern and significantly impacts my efforts to ensure the health information custodian is complying with access and privacy legislation, and to provide appropriate recommendations to the custodian aimed at preventing future breaches and encouraging improved compliance with the Act.

The key issues in this matter before me include:

1. Does the HIA apply and do I have jurisdiction?

2. Were reasonable measures in place and complied with to protect PHI?
3. Has NTHSSA responded appropriately to the breach?

ANALYSIS

1. Does the *Health Information Act* apply?

Pursuant to section 4 of the HIA, the Act applies to "all records containing personal health information that are in the custody or under the control of a health information custodian …".

The notice to my office identified that the breach was caused by an employee working for Frame Lake Community Health Centre (FLCHC), a clinic operated by the YK-Region of the Northwest Territories Health and Social Services Authority (NTHSSA) which is a health information custodian as defined in the HIA.

The information that was disclosed without authorization was about the health and health history of the individual and falls within the definition of personal health information as contained in the HIA.

I find that the FLCHC and staff are an operational body of the NTHSSA, and that NTHSSA is a health information custodian. The information that was disclosed in error was collected by the YK-Region for the purpose of providing health care to the patient and was in the custody or under the control of the NTHSSA. The *Health Information Act* therefore applies and I have jurisdiction to review this matter.

2. Were reasonable measures in place and complied with to protect personal health information?

The *Health Information Act* requires health information custodians to take reasonable steps to protect the personal health information they collect. Section 85 provides:

85.(1) A health information custodian shall take reasonable measures to maintain administrative, technical and physical safeguards for the protection of personal health information, including for protection

(a) of the confidentiality of personal health information and the privacy of individuals the information is about;…

(c) against unauthorized access to or unauthorized use, disclosure or alteration of personal health information;

In addition to section 85, subparagraphs 13(1)(j), and 13(2) of the regulations under the HIA require health information custodians to ensure that administrative, technical and physical safeguards are in place, to "provide for effective prevention... of privacy breaches" which are "proportionate to any threat to the security, confidentiality, or integrity of personal health information".

Further, as part of the administrative safeguards required under the regulations, a health information custodian is required to have policies in place to guide its administration and operations. Subsection 8(1) and (3) specifically state:

8.(1) A health information custodian shall establish or adopt standards, policies and procedures to implement the requirements of this Act and the regulations, including the requirements under sections 85 to 88…

(3) A health information custodian shall comply with standards, policies and procedures established or adopted under subsection (1).

In May 2019 I asked the Authority to provide me with more information about the breach, including policy and procedures in place for faxing and about staff education in privacy and information handling in place prior to the breach. I also asked why faxing was being used in this instance, and why a more secure means of communication was not employed. Despite this request for information, and several follow-up letters, in June and July, the Authority did not respond until August.

It was then that I was advised the employee involved in the breach had received "2010 clinical orientation" (I expect this means job orientation conducted in 2010), and mandatory privacy training in May 2018. In addition to this information, I also received a copy of an existing policy, an "Administrative Directive", entitled "Fax Transmissions… AD-030". This policy, AD-030, was originally created by the old Yellowknife Health and Social Services Authority, one of the several health authorities in the Northwest Territories amalgamated into NTHSSA in 2016. I received no explanation as to why faxing was used in this case.

Though my questions were about existing safeguards at the time of the breach, the Authority reported to me that all clinic assistants were sent the Administrative Directive (AD) with respect to fax transmissions via email on the 7th of February 2019, and the clinic assistant involved in the breach was sent another copy of it on February 14th. As proof of this the Authority offered that a "read receipt" was generated when the employee opened the email on the 14th. “Read receipt” or not, this was five months after the breach was "discovered". The breach occurred on or before October 1st, 2018. It is not at all clear that this protocol had been communicated to the staff at the time of the breach.

The Administrative Directive created by the YHSSA was last updated in December of 2012, and was scheduled for review and approval in December of 2014. Though old, the content of the it is still very applicable. It also seems that it has been adopted by the Yellowknife Region of NTHSSA in its current state in lieu of creating a new policy. Though the AD is relevant, I find it concerning, given the multiple and repetitive fax breaches, that the AD has yet to be reviewed, updated, translated into current format and approved by the Authority for use system wide.

Despite its age this AD is still relevant and helpful. According to the AD, "this protocol shall apply to **ALL** client and confidential administrative information, and **ALL** divisions/sections within the Yellowknife Health and Social Services Authority [bold capital as per original document]. It states that its purpose is to:

> reduce the use of fax transmissions as a mode of sharing information and to ensure that fax transmissions, when necessary, are used in a manner that protects the privacy of the information in question, and minimizes the risk of inadvertent delivery to unintended recipients.

The purpose of reducing the use of fax transmissions as a mode of sharing information is at the heart of this breach. The AD is clear that faxes are only to be used in limited situations. It states that only where specific criteria are met, including only where there is an "immediate" need, and "there is no other reasonably practical means of transmitting the information in a secure or timely manner", should faxes be used to transmit personal health information. Given this purpose, the AD was either not applied or is not robust enough to serve its stated purpose. I find the former to be the issue in this case as there is no evidence the employee was even aware of the AD prior to the breach. NTHSSA did not submit evidence that the AD was an active policy at the time of the breach or that it had educated its employees as to its content at the time of the breach.

The only additional safeguard mentioned in passing by the Authority was mention of pre-programmed fax numbers, in particular in relation to the DMV fax number. From this one might reasonably expect that the Authority has taken the time to pre-program often used fax numbers into the fax machine so that staff do not need to manually enter numbers. This should, in theory, reduce entry errors. In this case, however, the breach appears to have had more to do with the employee being in a rush - not manually clearing and/or not giving the equipment time to auto-clear the previous number.

This safeguard was in place at the time of the breach, so there were at least some fax related safeguards actually in operation. In addition, the Authority had the old YHSSA policy and although not reviewed and approved recently, if implemented, it might have prevented this breach. More secure means of communication are available and could have been used, as called for in the AD.

Unfortunately, there is no evidence that the employee who made the error (or any other employee) was aware of this policy. The employee, given circumstances at the time, was made to rush their work and this increased the risk of making mistakes. I find that there were no significant safeguards in place at the time of the breach, and as part of this, a lack of knowledge on the part of employees as to what protocols they should follow to protect privacy when considering the use of fax technology to transmit personal health information.

As a result, the Authority was not in compliance with sections 8 and 85 of the HIA or section 13 of the regulations. Nor in this case has the Authority adhered to its own policy, assuming that AD -30 remains an active policy. To the extent that it was active, AD -30 had not been reviewed and approved for several years and there were apparently no other tools or procedures to aid with employee compliance with this AD that might otherwise ensure the Authority could meet its responsibilities under 8(3) in its day to day operations.

3. Has NTHSSA responded appropriately to the breach?

A health information custodian is required by law to respond when a breach of privacy occurs with respect to records in its custody or control. Under section 14 of the HIA regulations, the following specifically is required:

> 14. A health information custodian shall
>
> (a) take reasonable steps following a security or privacy breach to investigate the breach and to ensure that a breach does not occur again;
>
> (b) keep a record of any security or privacy breach and any corrective measures taken as a result; and
>
> (c) take reasonable disciplinary measures against an agent who fails to comply with a provision of the Act, these regulations or any standard, policy, procedure or safeguard relating to

the Act or these regulations, having regard for

(i) the nature of the breach,

(ii) whether the breach was intentional or not, and

(iii) whether the agent has previously committed a breach.

In 2017, NTHSSA adopted a Privacy Breach Policy issued by way of a Ministerial Directive by the Department of Health and Social Services. This policy states: "this directive requires that the Department and HSSA staff follow the approved privacy standards, policies, and procedures referred to in this directive". As part of this directive, the Privacy Breach Policy requires the custodian to follow several steps in response to a privacy breach, including: initial reporting of the breach, investigation, notification, and response, including final reporting.

Initial Reporting and Investigation

The Authority provided very few details about the initial reporting and investigation of the breach, such as when or how the breach was discovered. Thus there were few clues to reflect the compliance of the Authority with the policy in terms of its initial reporting and investigation. Information provided by the Authority included that they discovered a lack of operating capacity had "significantly" contributed to the breach, that the employee was in a rush and failed to clear the last number they had used on the fax machine. There was reference to the DMV number being a pre-programed number, but not much other detail was provided.

I was told the breach occurred on or before the 1st of October 2018, this being the date the Authority "became aware" of the breach. Though my office was not notified until May of the following year, I suspect the initial investigation was conducted nearer the time the breach as required, rather than at the time my office was notified in May 2019. It is reasonable to conclude that the first part of the policy was somewhat complied with by the Authority, though the level of detail gathered seems rather wanting. The

requirement for investigation under 14(a) of the Act seems to have been met, though minimally, in this case.

Notice

According to the Privacy Breach Policy, as part of the response not only is an investigation required to be completed, but notice is to be provided to several stakeholders including my office and the individual affected by the breach, and this is to be done "as soon as reasonably possible". The expectation is that this notification will occur shortly after discovery of the breach and as soon as a basic understanding the nature of the breach and some conclusions about what can be done to prevent recurrence have been reached.

As discussed, the notice to my office was provided in May 2019. The Authority discovered the breach on October 1st, 2018. This does not constitute notice “as soon as reasonably possible” as required.

The Privacy Breach Policy states that the following is to be provided to the Information and Privacy Commissioner as soon as reasonably possible:

- where and when the breach occurred;
- the type of breach i.e. unauthorized use, disposal or disclosure, theft, loss;
- the media/form of information breached i.e. paper, electronic, verbal;
- the nature/subject of the information breached i.e. medical, mental health, child and family services;
- the type of documents/records of the information breached , i.e. patient chart, laboratory results, case notes;
- the number of individuals known or suspected who were affected and if or when they were or will be notified; and
- an overview of any immediate actions taken or changes made in response to/to mitigate/manage the breach.

Unfortunately, I was unable to elicit much of a response from the Authority, despite several requests over several months. Some details were provided in August, but those were still deficient. For example, it is still unclear when the breach actually happened or how it was discovered.

The Privacy Breach Policy contemplates that an even more extensive list of details about the breach is to be provided to the affected individual, including clearly identifying possible risks to the individual and how these risks might be best mitigated. Contact information for my office and the organization that caused the breach is also to be provided to the affected individual. Under section 87 the affected individual is also to be notified as soon as reasonably possible:

> 87. Subject to any prescribed exceptions, a health information custodian shall give notice to an individual and, if applicable, to a prescribed person or organization, as soon as reasonably possible if personal health information about the individual is
>
> (a) used or disclosed other than as permitted by this Act;
>
> (b) lost or stolen; or
>
> (c) altered, destroyed or otherwise disposed of without authorization.

Though the Authority states the affected individual was notified, I am not clear when they were notified. Nor is it clear what was included in the notice to the client.

The details and factors pertaining to a breach are important to gather in order to understand the nature of a breach, including its cause. These are key to the assessment of related risks, and to the breach response to ensure proportional and effective actions are taken given the circumstances. Without further evidence, it seems reasonable to conclude that many of the requirements of notice were met. However some details required to be provided were not provided, and rather importantly, the notice was not given in a timely manner as required by section 87.

Response

The Privacy Breach Policy requires both "immediate" and "long-term" mitigation measures be identified and implemented. According to the policy, immediate measures might include recovering the records, developing and implementing interim corrective measures, and providing on-the-job coverage or support. Long-term measures might include the development or delivery of additional training to staff and management, revising policies, directives, procedures, or standards, and/or revised administrative, technical, or physical privacy and security safeguards. The policy states that "The Department / HSSA must ensure long-term response measures respond to the root cause(s) of a privacy breach". The objective in all of this is, as per 14(a) of the regulations, to prevent a similar breach in the future.

As part of its response the Authority indicates that it "retrieved" the information from the DMV. As well, the Authority reported to me that "staffing levels have been reviewed, and continue to be monitored and addressed", and that "the faxing protocols [were] … reviewed with the staff involved", and that the same action was taken at a scheduled staff meeting with all staff.

It was not clear what "faxing protocol" was reviewed with staff and, if AD-30 was that “protocol”, whether there was emphasis on the use of faxing as a last resort, and/or if other more secure means of communication were identified and their use encouraged.

I asked the Authority, as part of the initial response, if the employee had received refresher training since the incident. Apparently no training was offered to them, but AD-030 was sent in February 2019 to all staff, and to the employee that caused the breach. The Authority added that a "read receipt" was logged for the email sent to the employee.

Positive steps were taken as part of the immediate response to the breach, but I am left to question why the AD was provided four months after the breach was "discovered",

and what on-going measures the Authority has put into place to ensure any employee does not make the same mistake.

Certainly revising, approving and actually implementing the administrative directive, would have been an appropriate long-term step, but that does not seem to have been done in this case. Nor is sending one email to staff an adequate long-term measure commensurate to the risk related to a breach if this kind. In particular, a “read” receipt does not ensure that the employee has read the protocol or understood its application. It merely confirms that an email has been opened. Simply emailing a policy (an outdated policy at that) to an employee does not meet the Authority’s responsibility under the Act to have safeguards in place.

I find the Authority’s initial response to the breach to be satisfactory, but that their long term response was wanting and not sufficient to prevent the breach from recurring, as is require under 14(a) of the Act. I will add that in light of the few details received from the custodian in response to my inquiries with respect to the breach, it appears that the recording of details required under 14(b) may not have occurred.

Response to OIPC and Final Reporting

Again with reference to 14(b) of the regulations and the Privacy Breach Policy under the Act, the policy recognizes the importance of providing information to my office about privacy breaches. The policy states: "If the IPC …. at any time requests information or specific records under HIA, whether there is a review or not, the Department/ HSSA must provide all the requested material." The breach notice and the response to my inquiries failed to identify the date on when the breach occurred, the date the individual was notified (though it is stated they were notified), and did not provide an adequate explanation as to why there was a seven month delay in reporting the breach to my office once the breach was discovered.

Among the information not provided to my office were important details including:

- when the breach occurred,
- if a fax cover page was used or not,
- how long it took between the time the fax was sent to the DMV and when the breach was discovered
- how the breach was discovered
- who reported the breach.

It is also unclear whether a final comprehensive breach report, as required by the Privacy Breach policy, has been completed. This report would have assisted with this review.

Disciplinary Measures

Knowing what caused a breach is important, as is the impact or outcome of the breach, when determining what corrective measures should be taken. There was no indication of a systemic issue or ongoing failure by this employee. This was not a breach caused by apathy or malice. It was a simple honest mistake caused in part by being in a rush. The clinic was understaffed and over-tasked at the time of the breach. Operating capacity is a management issue, and employees have little opportunity change this.

The response of the Authority was largely to review unidentified faxing protocols with the individual staff person, and all clinic staff at the next opportunity. AD-030 was sent around by email several months later. This seems to be the extent of the Authority's effort to correct the situation. Though the employee who made the error was likely unaware of the direction within AD-030, this staff person was not given follow up training as a means to correct the possible recurrence of the error, and I have no assurances that operations have changed to abide by the AD.

I do not consider this breach as one requiring discipline for the employee who made the error, particularly as it does not appear to be a repeated error. I do see it as an

indication that more privacy training is required.

CONCLUSIONS AND RECOMMENDATIONS

Notification to stakeholders about privacy breaches is important. Knowing the nature and details of a breach is critical to the accurate determination of risks posed to the affected individual and to identify possible actions that might mitigate risk and prevent future occurrences. This is also why transparency, accuracy and reporting to the affected individual and my office is important. The individual cannot assist themselves, and I cannot assist the Authority to improve legislative compliance if not notified in a timely and fulsome manner.

Though the Authority did obviously respond to the breach, the timeline of this response does not reflect the purpose or intent of the Act or the privacy breach policy. The measures in place before the breach were not sufficient to meet the need to protect personal health information and long term solutions were not identified.

I am particularly concerned about the ineffective operational response as it pertains to long term measures to prevent the breach from recurring, and to ensuring staff have the knowledge they need to protect privacy and work in an environment that in reality reflects existing administrative safeguards in place. In particular, there was no mention of management reviewing the AD-030 directly with their staff or the employee involved in the breach to ensure they understand that faxing is not to be used as a standard form of communication. Sending an email and receiving a ‘read’ receipt, and relying on this to fulfil the requirements of the Act with respect to administrative safeguards is not sufficient. Given the frequency of breach reports from the health sector involving misdirected faxes, I am not confident that staff anywhere in the NTHSSA are aware of AD-030 or for that matter if it is intended to apply beyond the Yellowknife region.

More work needs to be done, including reviewing, revising as necessary, and approving the old 2012 AD, changing the business culture to support this approach, and

communicating and providing meaningful learning opportunities for staff to learn about AD-030.

I make the following recommendations:

1. I recommend NTHSSA ensure AD-030 (2012) is reviewed, updated (if required), and approved for use within the new NTHSSA as a whole;

2. I recommend that the NTHSSA pro-actively disclose the policies that support the provisions of the HIA as a way to improve the public's and staff's accessibility to these polices;

3. I recommend that alternate means of communication that provide timely service and safe transfer be identified, and that practical process and procedures for staff to use these alternate tools be created and meaningfully communicated so that staff actually can reduce use of faxing as required in the policy;

4. I recommend that NTHSSA ensure that mandatory training includes:
   i. review of key policies that protect privacy;
   ii. review of clear protocols for avoiding faxing except when necessary;
   iii. review of a clear protocol for use of fax technology when necessary;

5. I recommend that the NTHSSA ensures any AD, policy, or procedure, once approved:
   - remains in force until next reviewed;
   - clearly identifies the responsible approver's position;
   - includes a fixed review date within a reasonable time period;
   - is brought forward for review on that date.

6. I recommend the Authority have all unit managers read the DHSS Privacy Breach Policy. Though I do not agree with some of the direction given in this

policy, it is a useful guide and should aid in ensuing basic steps are followed for breach responses.

7. I recommend that notification to my office and to affected individuals be made "as soon as reasonably possible", which means very shortly after a breach occurrence. Sufficient detail should be included in those notices for a reasonable person to have a good understanding of where and when the breach occurred, how it was discovered, what the immediate and underlying causes were, and provide some clarification on major safeguards in place at that time.

8. I recommend that for all breaches, the Authority complete and provide a fulsome privacy breach report including a full details and timeline of events, as soon as reasonably possible. For a relatively non-complex breach that should reasonably occur within 4 weeks of the discovery of the breach, if not sooner.

Elaine Keenan Bengts
Information and Privacy Commissioner