NORTHWEST TERRITORIES
INFORMATION AND PRIVACY COMMISSIONER
Review Report 20-248
Citation: 2020 NTIPC 55

File: 19-252-4 (6)
November 5, 2020

BACKGROUND

On October 22nd, 2019, my office received a notification from Northwest Territories Health and Social Services Authority (NTHSSA) - Stanton Territorial Hospital advising that they had received a complaint from a former employee about an unauthorized disclosure of his personal information. The former employee had been a patient at the hospital. He was advised by a former co-worker that there had been a casual discussion about his medical situation between two other co-workers in the presence of a number of other staff members, all of whom were also thereby made privy to information about the former employee's medical situation. None of the discussion was relevant to the affected individual's health care or the provision of health services to the affected individual.

NTHSSA's EXPLANATION

When the complaint was received, NTHSSA immediately determined the origin of the comments as being from one of the Complainant's managers. The manager admitted to having made an error in disclosing information about the Complainant's medical situation to co-workers and took responsibility for the error. The disclosure was not malicious or intended to harm the Complainant in any way. Rather, it was really more in the realm of office gossip about what amounted to good news about the Complainant's health status that the manager wanted to share with his co-workers. The manager had access to the information in question because it had been shared with the manager by the affected employee in the course of advising the manager that he would not be able to work certain shifts and that the manager needed to make arrangements for necessary personnel adjustments.

NTHSSA indicated that they determined that the cause of the incident was the manager's lack of knowledge on protecting the privacy and confidentiality of staff and patients who access care at Stanton Hospital. The manager was required, as a result of this incident, to complete Stanton's new privacy and confidentiality education modules which include the following topics:

a) General Privacy and Confidentiality
b) Privacy Safeguards
c) Respecting Patient Privacy
d) e-Health Privacy Awareness
e) Privacy Breach and Investigation
f) Access to and Correction of Health Information
g) Complex Consent under the *Health Information Act*
h) *Health Information Act* Overview, and
i) The Designated Contact Person

Staff in attendance at the meeting in which the conversation took place were all reminded about the requirement to safeguard clients' private health information.

DISCUSSION

Important context in analyzing this case is determining whether the applicable legislation is the *Access to Information and Protection of Privacy Act* or the *Health Information Act*. In either case, I think the conclusions are very similar, but it is important to know which piece of legislation applies. Here, the information that was discussed by the manager with his colleagues in a particular work group was not information that was collected by the manager in his role as a health care provider. It was information given to a manager of a public body in the context of personnel management. While it was information about the affected employee's health, it was not personal health information as defined in the *Health Information Act* because it was not collected in the context of the provision of health services.

Section 4(1)(d) of the *Health Information Act* recognizes that in this case, the *Health Information Act* does not apply:

> 4.(1) This Act applies to all records containing personal health information that are in the custody or under the control of a health information custodian, except the following:
>
> ...
>
> (d) a record containing personal health information about an employee or agent of the custodian that is not made or maintained primarily for the purpose of providing or assisting in the provision of a health service to the employee or agent;

The *Health Information Act* does not, therefore, apply to the information in question. The information was about an employee of the custodian that was not provided for the purpose of providing or assisting in the provision of a health service to the employee. Rather, it was provided for the purpose of allowing the manager to address personnel issues.

NTHSSA however, is also a public body as defined in the *Access to Information and Protection of Privacy (ATIPP) Act*. It must, therefore, also comply with this legislation in relation to the personal information that it collects, uses and discloses in relation to matters not covered by the *Health Information Act*.

Section 2 of the *Access to Information and Protection of Privacy Act* defines personal information as follows:

> “personal information" means information about an identifiable individual, including
>
> ...
>
> (f) information about the individual’s health and health care history, including information about a physical or mental disability,

Information about the affected employee's health status clearly meets the definition of personal information under the ATIPP Act.

Section 47.1 of the ATIPP Act imposes a duty on the employees of all public bodies to refrain from disclosure of personal information which the employee becomes aware of as a result of his/her employment:

> 47.1. An employee shall not, without authorization, disclose any personal information received by the employee in the performance of services for a public body.

The information about the employee's medical status received by the manager was information he had received in his role as a manager and in the performance of his employment with the public body. He was, therefore, bound not to disclose the information he became privy to "without authorization".

Section 48 of the ATIPP Act outlines those circumstances in which a public body (or an employee of a public body) **may** (not must) disclose personal information about an individual - in other words, circumstances in which disclosure is "authorized". Those purposes include the purpose for which the information was collected or compiled or for a use consistent with that purpose. The information in this case was collected for the purpose of allowing the public body to manage its workforce and ensure appropriate personnel was available to cover the gap left by the affected employee's absence. The information was not intended for the purpose of advising one or more fellow employees and co-workers about the affected employee's health status. Neither was this a consistent purpose.

Section 48 also allows for the disclosure of personal information where the person the information is about has consented to the disclosure. Clearly there was no consent in this case.

Subsection 48(g) does allow for the disclosure of personal information "for the purpose of hiring, managing or administering personnel of the Government of the Northwest Territories or a public body". That, in fact, is why this information was collected. However, in this case, it is conceded by the manager and by NTHSSA that this was not the context of the disclosure. Section 48(g) did not apply so as to result in an authorization to disclose the affected employee's personal information.

Section 48(k) allows for the disclosure of personal information to an employee of the public body where the information is necessary for the performance of the duties of the employee. In this case, the individuals to whom the information was disclosed had no operational or work related need for information about the affected employee's health situation.

None of the other circumstances in which the disclosure of personal information is allowed as enumerated in section 48 could be said to apply to this disclosure.

I find that the disclosure of the affected employee's personal information to his co-workers by the manager was an unauthorized disclosure under the ATIPP Act.

NTHSSA's RESPONSE

In this case, the manager quickly recognized that he had made a mistake by disclosing the information about his employee to other co-workers and owned up to the mistake. That said, I do not entirely accept the suggestion that the manager lacked knowledge about protecting the privacy and confidentiality of staff and patients when he disclosed the affected employee's information. Rather, I believe this was more in the nature of a slip in application of clear and known protocols. I can understand why it happened - it is hard not to share good news affecting co-workers. It is because it is easy to understand why it happened that NTHSSA and its employees must be that much more diligent to protect personal information of its employees as well as of its clients.

I am also satisfied that the steps taken by NTHSSA to control and deal with the breach were appropriate, though not entirely adequate.

This event occurred in sometime between September 11th (the date on which the affected employee provided the manager with the information) and September 16th (the date on which the affected employee complained to NTHSSA). My office was notified of the breach on October 22nd. I note that at the time of this preliminary breach report, NTHSSA had indicated that they intended to formally notify the affected employee of the breach. On December 19th, when I received NTHSSA's Final Breach Report, it appeared that the affected employee had not yet received a formal letter from NTHSSA outlining specifically what information had been inappropriately disclosed, what steps were being taken to address the breach or advising the affected employee that he could request the Office of the Information and Privacy Commissioner to review the unauthorized use/disclosure of his personal information.

While the ATIPP Act does not specifically require that individuals be notified of unauthorized collection, use or disclosure of personal information at this time, I suggest that it is a matter of good privacy breach management and, if nothing else, the right thing to do. It should be noted that breach notification will become a mandatory part of breach management when Bill 29 - *An Act to Amend the Access to Information and Protection of Privacy Act* comes into effect. It is already a requirement under the GNWT's Privacy Breach Policy which I understand to have come into effect in August, 2019 and under the *Health Information Act* and the Privacy Breach Policy of the Department of Health and Social Services.

I **recommend** that NTHSSA establish and implement a protocol to address unauthorized collection, use and disclosure of personal information under the *Access to Information and Protection of Privacy Act*, which would include a requirement to notify an affected individual of the breach. The information to be included in such notice should specifically include:

- where and when the unauthorized collection, use, disclosure 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 inappropriately collected, used or disclosed etc.(i.e. medical, mental health, child and family services);
- the type of documents/records of the unauthorized collection, use disclosure , i.e. patient chart, laboratory results, case notes;
- Risk(s) to the individual caused by the unauthorized collection, use, disclosure, if applicable and known;
- an overview of any immediate actions taken or changes made in response to/to mitigate/manage the breach;
- a commitment to take future steps to prevent further unauthorized collections, uses and disclosures of personal information;
- steps the individual can take to further mitigate the risk of harm (e.g. how to contact credit reporting agencies to set up a credit watch if applicable);
- contact information of an employee with the organization who can answer questions or provide further information; and
- Information and Privacy Commissioner contact information and the fact the individuals have a right to ask for a review by the Information and Privacy Commissioner.

Alternatively, NTHSSA should expand the application of its Privacy Breach Policy in relation to the handling of personal health information under the *Health Information Act* to its handling of personal information under the *Access to Information and Protection of Privacy Act.*

It is also of some concern here that, while there were apparently a number of employees present who heard or were privy to the discussion about the affected employee, none of these employees reported the unauthorized disclosure to the appropriate authority. At least one employee present in the room, however, recognized the conversation as constituting a breach of privacy as they reported it to the affected

employee. The affected employee, therefore, heard about the breach from a co-worker rather than from the NTHSSA and was required to file a complaint about the incident in order for it to be addressed. Employees, particularly those who work in the health sector and are subject to the *Health Information Act* as well as the *Access to Information and Protection of Privacy Act* should be clear about the necessary and appropriate steps that should be taken when they become aware of an unauthorized collection, use or disclosure of personal information or personal health information. I therefore **recommend** that NTHSSA take steps to ensure that all employees are aware of their obligations to report breaches of privacy of which they become aware to the Quality Risk Manager of the appropriate region. This apparently needs to be communicated more than once a year during privacy training. I would recommend that it become part of regular monthly or even weekly messaging sent to all employees.

I note, as well, that prior to this privacy breach the last privacy training that the manager had participated in was in December, 2014. The Department of Health and Social Services' Privacy Training Policy, which applies to the NTHSSA, requires annual training in privacy issues. This policy is clearly not being adhered to. While in this case, the manager has now received additional training, there is no indication that any of the other employees involved (those who heard the disclosure but failed to report it) have also been required to complete additional training. I do applaud the organization for their efforts to produce additional privacy training modules and encourage them to continue to update and add new modules to the available training. More, however, has to be done by NTHSSA to ensure that its employees complete the required annual training. I **recommend** that NTHSSA establish and implement a way to enforce the requirement for annual training, with consequences for failure to complete the training including the withdrawal of access to the EMR and other medical records.

Elaine Keenan Bengts
Information and Privacy Commissioner