NORTHWEST TERRITORIES
INFORMATION AND PRIVACY COMMISSIONER
Review Report 20-235
Citation: 2020 NTIPC 35

File: 19-228-4
July 10, 2020

BACKGROUND

The Complaint in this case asked us to review a breach of his privacy which had been reported to him by the Workers' Safety and Compensation Commission. The WSCC reported to the Complainant that correspondence and a redacted investigation report intended to be sent to him had been sent, instead, to an incorrect email address by an employee. An attempt was made to recall the message when the error was discovered, but they could not verify that this was successful. The WSCC also attempted to contact the actual recipient to request that the mail and its attachments be deleted and to emphasize the confidential nature of the documents sent in error, but they were unable to verify contact with the recipient.

THE WSCC'S EXPLANATION

The WSCC admitted the error which resulted in an email and attachments containing the personal information of the Complainant, a former employee of the WSCC, being directed to the wrong email address. Attached to the email was a report communicating the findings of an investigation conducted by the Department of Finance, Labor Relations, GNWT in response to a complaint submitted by the Complainant against the WSCC under the GNWT *Harassment Free and Respectful Workplace Policy*. The report had been redacted to remove third party personal information. The attachment had not been password protected or encrypted.

The Complainant's email address did not contain his name as an identifier, but a pseudonym. When typing the address, the WSCC employee apparently misspelled the pseudonym. They indicated that they could not confirm that the email was actually in

use by a third party, though no notice was received indicating that the email was undelivered or undeliverable.

The breach was discovered when the Complainant, who was expecting to receive a copy of the investigation report, contacted GNWT Human Resources to find out when it would be available. NWT Human Resources, in turn, contacted the WSCC to find out when they would be able to send it to the Complainant. At that point, the individual who had sent the email checked the address and discovered the error. Steps were immediately taken in accordance with the WSCC's breach response protocol, including contacting the ATIPP Coordinator for the organization, who took responsibility for follow up. The Complainant was advised of the error the following day. There were several attempts to contact the unintended recipient through the email address used in error, but no response was received and there was no way to verify who the owner of the account was, or in fact, if the account even existed.

The investigation report was subsequently sent to the Complainant through a secure file transfer portal.

The WSCC indicated that it did not currently have a policy related directly to encryption or secure file transfer. They did, however, point to their Administrative Policy A.4 (Internal Records Security) which outlines employees' responsibilities regarding privacy and confidentiality. They also advised that a procedure for utilizing a secure file transfer protocol was in the late stages of development. This system, when functional, will provide secure file transfer capabilities through an encrypted and password protected online drop-box system.

DISCUSSION

The WSCC is a public body that collects, uses and discloses large quantities of personal information and personal health information. Section 42 of the *Access to Information and Protection of Privacy Act* requires public bodies to protect personal

information in its custody and control from unauthorized use and disclosure:

> 42. 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.

Section 47.1 adds to that responsibility in terms of the responsibility of employees of public bodies:

> 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.

In this case, the WSCC cannot verify whether anyone has actually received the email containing the Complainant's personal information. Was there a breach if there was no "recipient"? In my opinion, if there is a possibility, verifiable or not, that the information might be seen by someone not authorized to see it, the public body has failed to comply with their obligation to protect the information from unauthorized use or disclosure. The public body has lost control of information which was their responsibility to keep protected. The misdirection of the email containing the Complainant's personal information therefore constitutes a breach of his privacy.

I am satisfied that the steps that WSCC took in reaction to the breach were appropriate. They acknowledged the breach quickly and took steps to ensure that the Complainant was informed. They took what steps they could to recall the email and to follow up with the unintended recipient. Unfortunately, those efforts were not successful.

Where the WSCC failed in this case is in the failure to have adequate policies and procedures in place to protect personal information and the failure to use appropriately secure means of communication. As an organization that collects, uses and discloses significant amounts of personal information and personal health information, one would

have expected that they would have a clearly set out policy for secure communications, which would include the use of passwords and/or encryption to protect any communication containing personal information which, if disclosed to a third party, would amount to an unreasonable invasion of privacy. It appears from the information received from the WSCC in response to this review that a system is being implemented (and may have been implemented by the time this report is issued) but it is unclear why this kind of protection has not been in place for years. Having the appropriate tools, including relevant policy and procedure, is part of privacy best practice.

RECOMMENDATIONS

Once information has been inappropriately disclosed, there is no way to undo that error. What we can do, however, is to learn from the errors made so as to avoid similar breaches in the future. To that end, I make the following recommendations:

1. I recommend that the WSCC acquire and require the use of a secure messaging platform when communicating with clients and others where the communications include sensitive personal information. There are any number of such platforms available for purchase or license on the market. Whichever system chosen by the organization should be subject to a detailed privacy impact assessment before implementation.

2. I recommend that, until such time as this platform is installed and ready for use, and in situations in which the secure messaging platform cannot, for some reason, be used that the WSCC require that all digital communications with clients and/or employees be encrypted or password protected where the communication contains personal information, the disclosure of which might result in an unreasonable invasion of the client's or the employee's privacy.

3. I recommend that the WSCC develop and implement a clear policy for appropriately secure communication with clients and employees, including

priority use of various means of communication (i.e. secure messaging platform, encrypted email, password protected attachments, registered mail etc) which recognizes that while most business is now done digitally, there may be situations in which digital communication is not appropriate.

Elaine Keenan Bengts
Information and Privacy Commissioner