ᓄᓇᕗᒻᒥ ᑐᓴᐅᒪᔪᓕᕆᓂᕐᒧᑦ ᑲᓐᒍᓇᖅᑐᓕᕆᓂᕐᒧᓪᓗ ᑲᒥᓯᓇ
Nunavut Information and Privacy Commissioner
Commissaire à l’information et à la protection de la vie privée du Nunavut

Commissioner’s Final Report

Report Number:	21-183
CanLII Citation:	Department of Health (Re), 2021 NUIPC 2
NUIPC File Number(s):	20-149-5
Date:	January 28, 2021

Summary

[1] Two Department of Health managers had an e-mail exchange concerning the availability for work of a departmental employee.[1] The exchange included aspects of the employee’s medical care that should have been confidential. A supervisor recognized the breach of privacy but had to make several interventions before the breach stopped. The Commissioner finds there was a breach of the employee’s privacy, but that the Department of Health took appropriate steps to respond to the breach.

Nature of Review and Jurisdiction

[2] This is a privacy breach review, initiated by the Commissioner pursuant to s 49.1(2) of the Access to Information and Protection of Privacy Act (ATIPPA). The employee concerned was notified of the potential breach by the Department of Health, and also of the right to seek review from this office, but did not request a review pursuant to s 49.1(1).

---

[1] For the purpose of anonymization, it is the Commissioner’s practice not to name GN employees, other individuals or communities unless the names are relevant to an understanding of the issues; and also to use the pronouns “they/them” even when referring to an individual.

[3] The Commissioner has jurisdiction over the Department of Health: ATIPP, s 2, definition of "public body". The Commissioner may initiate a review, even in the absence of a complaint: ATIPPA, s 49.1(2).

Issues

[4] The issues in this review are:

a. Was there a breach of the employee's privacy?
b. If so, did the Department of Health take appropriate steps to respond to the breach?

Facts

[5] On April 8, 2020, over the course of a couple of hours, there was an e-mail discussion between two Department of Health managers (who I will refer to as Manager 1 and Manager 2) about the availability for work of a departmental employee.

[6] The discussion was occurring near the beginning of the COVID-19 pandemic, and there appears to have been some uncertainty about when an employee should or should not be at work.

[7] The discussion included details of the employee's health information, including medical appointments and test results. Some of the information appeared to come from a conversation with the employee's physician. It also included reference to others' opinions about the employee, as well as the employee's living arrangements and travel plans.

[8] At 1:43pm, a couple of hours after the e-mail chain started, Manager 2 copied it to two more senior managers, looking for direction.

[9] One of the more senior managers, who I will refer to as Supervisor 1, immediately recognized the privacy breach. At 2:14pm, Supervisor 1 wrote a "generic" (their word) e-mail to a number of employees, including Manager 1 and Manager 2, concerning client confidentiality and employers' responsibilities. This e-mail did not refer to the employee.

[10] At 2:24pm, Manager 1 wrote another e-mail to Manager 2 about the employee, continuing the previous conversation.

[11] At 2:30pm, Supervisor 1 wrote another e-mail directed specifically to Manager 1 and Manager 2, and specifically referencing the employee: "Hi all. Please STOP communicating specific client information. This is breaching the client's right to privacy and confidentiality. Employers do not have any right to know diagnosis, treatment or any monitoring employees are receiving at the health centres."

[12] At 3:04pm, Manager 1 wrote another e-mail to Manager 2 about the employee, continuing the previous conversation.

[13] At that point, the relevant e-mails stop. It appears that Supervisor 1 may have picked up the phone to speak to Manager 1, with the result that Manager 1 acknowledged the problem and agreed verbally to stop writing about the employee's confidential medical information.

[14] Supervisor 1 then reported a privacy breach to the central office of the Department of Health. The Department, having judged it was a material breach, notified the Information and Privacy Commissioner pursuant to s 49.9(1) of ATIPPA. The Department also notified the employee of the breach. The notification letter informed the employee of the right to seek review by the Information and Privacy Commissioner. The employee did not seek review.

[15] On April 25, 2020, the Commissioner wrote to the Department of Health, indicating her intention to initiate a review under s 49.1(2), and seeking further specific information.

[16] On June 17, 2020, the Department of Health wrote to the Commissioner with answers to the Commissioner's questions.

Law

[17] "Personal information" means any information about an identifiable individual, including information about their health or health care history: ATIPPA, s 2.

[18] Personal information may be disclosed only in accordance with the access provisions (which do not apply here) or sections 48, 48.1 or 49: ATIPPA, s 47.

[19] Personal information may be disclosed "for the purpose for which the information was collected or compiled or for a use consistent with that purpose": ATIPPA, s 48(a). Section 48.1 explains further what "consistent" means.

[20] Personal information may also be disclosed "for the purposes of hiring, managing or administering personnel of the Government of Nunavut…": ATIPPA, s 48(g).

Analysis

[21] This is a case in which two Department of Health managers impermissibly blurred the line between what they knew as personnel managers, and what they knew because they worked in a health setting. They should have kept those two roles separate, but they did not.

The privacy breach

[22] Manager 1 and Manager 2 were entitled to discuss the management of the employee. That was part of their job.

[23] However, Manager 1 injected into the conversation details of the employee's medical care, including medical appointments and test results. These details should have been known and discussed only by and between the employee's direct care providers and only for the purpose of providing health care services to the employee. Manager 1 appears to have learned

some of the details of the employee's care from the employee's doctor, without the employee's knowledge or consent.

[24] A patient is entitled to privacy with respect to the patient's medical care. An employer is not entitled to know the details of an employee's medical care, except for limited purposes authorized by law, e.g. sections 25(5) and 164 of the *Workers' Compensation Act*, SNu 2007, c 15.

[25] The fact that the employee worked for the Department of Health does not change their right to privacy. The fact that Manager 1 and Manager 2 were Department of Health managers, and therefore might have information not available to other employers, did not change their obligation to respect the employee's privacy.

The Department's response

[26] Because the breach of privacy is obvious, the main purpose of this review is to ascertain whether the Department of Health took appropriate steps to deal with the breach. In my view, they did, although I still have some recommendations for further action (see the Recommendations section at the end of this report).

[27] In general, a public body that learns of a privacy breach within the organization has a four-step obligation: contain the breach; notify those affected by the breach; investigate the breach; and take adequate steps to prevent future, similar breaches.

Supervisor 1

[28] Once looped into the e-mail exchange, Supervisor 1 acted immediately and appropriately.

[29] Supervisor 1 first responded with an e-mail of "generic" guidance. For educational purposes, I repeat it here almost in full:

> *…I would like to remind you all it is important to respect the privacy and confidentiality of all clients. It is important to only*

share client specific information with those directly involved in the circle of care.

…It is important to separate your professional nursing role and your supervisory/employer role. As employers, you are not entitled to know specific client health information, [any more than] any managers in the GN in different departments.

Employers Role/Supervisor Role:

1. Employers do not have the right to know the diagnosis of employees, consent must be provided

2. Employers do not have the right to even know that clients are being medically monitored or treated at the health centre, consent must be provided

3. Employees themselves, determine what medical history they share with their supervisor/employer

Healthcare Provider Role:

1. Only share client specific information with those directly involved in the circle of care

2. Respect the client's right to privacy and confidentiality

3. Follow directions of the [Chief Public Health Officer's] office regarding COVID19.

[30] This generic guidance was sent to eight employees, including Manager 1 and Manager 2, and was copied to two directors superior to Supervisor 1.

[31] Perhaps because this e-mail was widely circulated, Manager 1 may not have understood that it was prompted by the e-mail exchange with Manager 2. Perhaps Manager 1 did not read it. In any event, ten minutes later Manager 1 resumed the e-mail conversation with Manager 2 about the employee.

[32] Supervisor 1 responded within minutes, this time with an e-mail directly to Manager 1 and Manager 2, and specifically referencing the employee. This e-mail could not have been misunderstood by Manager 1.

[33] Inexplicably, Manager 1 then continued the e-mail conversation about the employee with Manager 2. When that was brought to Supervisor 1's attention, it appears Supervisor 1 then communicated directly with Manager 1, probably by phone. The e-mails stopped and there was no further breach of the employee's privacy.

[34] Supervisor 1 knew the rules, recognized the breach immediately, acted on it immediately in a constructive but firm way, and stayed with it until the breach was stopped. Supervisor 1 then promptly filed a privacy breach report with the department's central office. Supervisor 1 did everything right.

The Department

[35] After the Department received the privacy breach report from Supervisor 1, it notified the Commissioner and notified the employee. It responded within a reasonable period, including an extension granted by the Commissioner, to the Commissioner's questions.

[36] The Department acknowledges that it may have been as long as 10 years since Manager 1 and Manager 2 had any privacy training. Nobody is sure. The former Commissioner has recommended, in review reports too numerous to list, more and better privacy training for GN employees. The need is particularly acute for health employees, who are handling such sensitive, personal information.

[37] Privacy training is not a panacea. Some employees will understand privacy implicitly, whether or not they receive specific training. Some employees will not understand privacy, no matter how much training is offered. Our objective is to develop a privacy culture in which everybody feels responsible and empowered to protect citizens' privacy. This is of special and utmost importance in the health-care sector. A privacy culture, like a

safety culture, is more likely to be developed if training and reinforcement is woven into the fabric of the workplace. If one person slips up, another will be there to catch it and correct it.

[38] The root of the problem in this case is that Manager 1 and Manager 2 seemed oblivious to their breach of the employee's privacy. I am not quite prepared to say that they did it intentionally; I do not know what was gong on in their heads. They should have known better. Supervisor 1 did know better, and acted on it by sending first a generic e-mail and then a specific e-mail directing them to stop. At that point, Manager 2 seems to have "got the message". Manager 2 continued to receive e-mail from Manager 1 about the employee, but did not reply.

[39] The conduct of Manager 1 in this case leaves much to be desired. Manager 1 continued to breach the employee's privacy even after a generic, then a specific, directive from Supervisor 1 to stop. I do not think this is a training issue, or not primarily a training issue. This is a disciplinary issue. It is not within my mandate to recommend employee discipline, but I can recommend the department consider it. The documentation on file suggests that the Department understood the seriousness of Manager 1's misconduct and there may already have been disciplinary consequences.

The doctor

[40] Some of the information shared between Manager 1 and Manager 2 appears to have come from a conversation between Manager 1 and the employee's doctor. This was a serious lapse by the doctor. According to the Department of Health, the doctor later contacted and apologized to the employee. Assuming that to be a fact, I trust the doctor is suitably chastened. With or without specific privacy training, doctors know better than to discuss patients with someone not involved in their medical care. Acknowledgements of error and apologies are to be encouraged. I do not recommend further action concerning the doctor.

Conclusion

[41] There was a breach of the employee's privacy contrary to the ATIPPA.

[42] The Department of Health has taken appropriate steps to deal with the breach of privacy. Supervisor 1 contained the breach, though it took more effort than should have been necessary. The department notified the person affected by the breach, and investigated the breach. I am satisfied that the department has learned from the incident and taken sufficient steps to ensure a breach of this kind will not be repeated.

Recommendations

[43] **I recommend** that this report be shared by the Department of Health with (at least) Manager 1, Manager 2, Supervisor 1, and the doctor, if they are still employed within the GN.

[44] **I recommend** that the Department of Health consider disciplinary action against Manager 1, if it has not already done so.

[45] Because the employee did not seek a review under ATIPPA, even after being advised of the right to do so, I do not have their contact information. **I recommend** that this report be forwarded by the Department of Health to the employee, if the Department has the employee's current contact information.

[46] Although Manager 1 and Manager 2 may not have received any privacy training within the past 10 years, which is a matter of concern, I am not persuaded this case is primarily a training issue. I therefore do not make a recommendation about training.

Graham Steele
ᑲᒥᓴᓇ / Commissioner / Kamisina / Commissaire