# NORTHWEST TERRITORIES
# INFORMATION AND PRIVACY COMMISSIONER

Review Report on OIPC File 23-565-4

Citation: Re Department of Education, Culture and Employment, 2023 NTIPC 38

November 23, 2023



**SUMMARY**

An unknown intruder broke into a public body's office building and stole a hard drive containing personal information of almost 3000 people. Paper client records were in plain sight in the work area, and the intruder rifled through unlocked drawers and cabinets. The public body discovered the breach some hours later and took steps to investigate, give notice, and prevent future incidents. The Commissioner found that the public body failed in its duty to protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal. The Commissioner made recommendations to prevent future incidents.

**BACKGROUND**

[1] At 2:46 am on March 16, 2023, someone broke into a Yellowknife office building where the Department of Education, Culture and Employment (ECE) had offices. ECE employees noticed the break-in when they reported for work several hours later.

[2] While in the building, the person accessed a workspace used by the Income Security Program. Office doors, cabinets and desk drawers had been left unlocked. The person rifled through offices in the Income Assistance and Student Financial Assistance areas and stole keys, personal items belonging to staff, and electronics owned by the public body.

[3] The intruder stole two cell phones. One was relatively new and was protected by a password. The other was a device from 2018 that had previously been deactivated; the public body cannot confirm what was on it.

[4] A total of 79 client paper files were in plain view atop staff desks or in the identified unlocked drawers and cabinets. No paper files were identified as missing, but the public body was not able to determine whether the personal information in these files had been accessed or copied.

[5] The intruder also stole five small portable hard drives. One was brand new, still in the packaging and three were blank. The final portable hard drive, not used in several years, contained a copy of a file folder from the secured network drive. The folder

contained the personal information of income assistance clients from 2006-2014: names, addresses, social insurance numbers, health care card numbers, records of payments made, and medical status. A total of 2987 individuals' personal information was breached when this hard drive was stolen.



**JURISDICTION**

[6] Section 49.1 of the *Access to Information and Protection of Privacy Act* (the Act) establishes the right of an individual to request the Information and Privacy Commissioner (the Commissioner) to review whether a public body has disclosed the individual's personal information in contravention of Part 2 of the Act.

[7] The Commissioner received several requests for a review of the incident. Copies of this report will be provided to each of those individuals.

**ISSUES**

[8] Did the public body protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, or disposal, as required by section 42 of the Act?

**DISCUSSION**

**History**

[9] Several years before the theft, an employee at the public body had copied a file folder from the secured network drive to the hard drive and then transported it home so they could work after normal business hours.

[10] The folder contained 2987 individuals' personal information. No steps had been taken to de-identify the data set or to protect the privacy interest in the information. No physical, technical, or administrative safeguards were used to protect the personal information contained on the hard drive. The information could be accessed simply by connecting the hard drive to a computer.

[11] At the time the personal information was saved to the hard drive, the employee was not aware of more secure methods to access files from off site.

[12] At the time of the break-in, years later, the personal information still remained on the hard drive. It was stored in an unlocked drawer in an employee's unlocked office.

[13] The public body had no ability to access the hard drive remotely after it was stolen and so was unable to remove the information or prevent access to it.

**Personal information on the device**

[14] The personal information saved to the hard drive had been used for two projects. The first was an evaluation of childcare allowances provided to low-income families. The second was a review of cases where previous reviews had showed clients had received larger payments than they were entitled to. Although somewhat dated, this is potentially very sensitive personal information and could potentially be used to pursue fraudulent activities involving identity theft.

[15] The personal information had been collected years before the theft. At the time, clients signed a Statement and Authorization each year consenting to the collection of their personal information and allowing the information to be shared between programs run by the public body.

[16] Public bodies have a need to collect and use personal information to manage their programs and services. The Income Assistance Program provides financial assistance to NWT residents to help meet their basic needs. Its goal is to ensure clients have the opportunity to develop greater financial security so they are able to participate in community life and share in opportunities throughout the territory. Staff at the program assess applications, applying the *Social Assistance Act* and the Income Assistance Regulations. This involves collecting and reviewing large amounts of personal information about clients and their dependents.

[17] Section 40 of the *Access to Information and Protection of Privacy Act* says:

> 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
>
> (ii) a proposed program or activity where collection of the information has been authorized by the head with the approval of the Executive Council.

[18] The public body provided copies of the "overpayment recovery agreement" form that was in use in 2014 and the one that replaced it in 2018. The 2014 form collected social

insurance numbers, and the 2018 version did not, reflecting the public body's eventual determination that this category of personal information was not necessary for an existing program or activity.

[19] The Income Assistance Regulations have been amended over the years, also reflecting an awareness that some categories of personal information that were previously collected are not necessary for an existing program or activity. This is encouraging, and public bodies should continually review and assess whether the information they collect relates directly to and is necessary for existing programs or activities.

[20] The public body clearly has a need to collect personal information, including financial information, from its clients in order to administer the Income Assistance program. Once collected, the public body has a duty to make reasonable security arrangements to ensure there is no unauthorized access or disclosure of the information.[1]

**The stolen records were duplicate records.**

[21] The hard drive was a backup of a specific folder that remained on the GNWT shared drive. The public body was able to re-create the exact files from the network drive. Therefore, the records on the hard drive were duplicate documents: records that duplicate a master record and that were created for ease of reference.

[22] The Government of the Northwest Territories' Records Disposition Authority 1997-02 is intended to govern the disposition of transitory records. Under the Disposition Authority, duplicate records are considered to be transitory when they are no longer required for reference purposes. Transitory records are to be destroyed when no longer required.

[23] Copies on the hard drive should have been destroyed when the two projects were completed, leaving the master copies secure on the network drive. The public body's failure to destroy these duplicate copies of large amounts of personal information, and the failure to make reasonable security arrangements led to a significant privacy breach. The security arrangements for the personal information on the hard drive should have been similar to the security arrangements for the personal information on the network drive. Unfortunately, it wasn't; the most one might say is that the information was stored out of sight.

[24] I have not reviewed the security arrangements for the network drive used by ECE, as that is somewhat beyond the scope of this review. Any comment here should not be taken to endorse the sufficiency of the security arrangements regarding the public

[1] Per section 42 of *Access to Information and Protection of Privacy Act*

body's computer system. Rather, this event and this review should be taken to be a firm reminder of the obligation under section 42 of the Act, and that "reasonable security arrangements" need to be continually reviewed and assessed and updated as required by circumstances.

**The theft involved a material breach of privacy that created a real risk of significant harm.**

[25] Sections 49.7 to 49.10 of the *Access to Information and Protection of Privacy Act* require notice to the Information and Privacy Commissioner in the event of a "material breach of privacy" and notice to any affected individual in the event that a privacy breach creates a "real risk of significant harm." "Harm" is a defined term:

> 49.7. In this Division, "harm" includes bodily harm, humiliation, damage to reputation, damage to a relationship, loss of an employment, business or professional opportunity, a negative effect on a credit record, damage to or loss of property, financial loss and identity theft. SNWT 2019, c.8, s.34.

[26] The personal information on the lost hard drive or on the unsecured paper files included client names for 3066 individuals, spouse and dependent names, mailing addresses, financial information, social insurance numbers and personal health numbers. This is the type of information that could be used to cause financial loss or identity theft. It could also cause humiliation or damage to reputation. Given the sensitivity of the stolen personal information, the number of individuals who were affected, and the likelihood of harm to those individuals, I conclude the theft involved a material breach of privacy under section 49.9.

[27] There is no evidence that the stolen personal information has been or is being misused. The public body has received no reports from individuals or from the police investigation that there has been any identity theft or financial loss ensuing from this event. However, this is not a guarantee that the information will not be misused in the future. Combined with the sensitivity of the personal information that was breached, I concluded that the theft created a real risk of significant harm under section 49.10. As described below, the public body provided the affected individuals with the required notice.

**The public body's response after the breach was appropriate.**

[28] Following the break-in, the public body immediately took steps to determine the scope of the breach, notify clients, and update practices to prevent future breaches.

[29] The public body discovered the breach a few hours after the break-in when staff reported for work. It notified the property owner, the RCMP, and the Information and Privacy Commissioner. It notified all building staff and provided reminders about building access and safety protocols. It notified internal GNWT corporate support offices and reported the breach to the Canada Revenue Agency. Staff created a fob inventory, moved all spare keys to a secure area, and deactivated credit cards and a bank token. All electronic key fobs were accounted for, and a process was implemented to ensure that employees' fobs are deactivated once they no longer work in the building. An employee re-created the information that was on the hard drive and compiled a list of clients whose personal information had been breached.

[30] Section 49.10 of the Act required notice to all 3066 affected individuals of the breach of privacy with respect to their personal information under the public body's control.

[31] Seventy-nine current client files were unsecured on staff desks or in unlocked drawers or cabinets. These clients received an email notification on March 28, 2023.

[32] Notification for the clients named on the hard drive proved more challenging. The personal information had been collected years earlier, and in some cases was out of date. Because some of the clients were no longer living at their listed addresses, it is not possible to confirm that all of the clients whose personal information was stolen were made aware of the breach.

[33] Of the 2987 clients named on the hard drive, 2574 had addresses listed. Notification letters were mailed to these addresses during the week of April 12, 2023. Some letters were returned as undeliverable; where the public body had secondary addresses on file, these letters were re-labelled and sent out again. Public service announcements on social media continued from April 19-26, 2023 to advise the remaining clients and the public of the breach. These notifications included contact information for a manager who could answer questions. As previously noted, several individuals requested the Commissioner to review the public body's breach of their privacy.

[34] Since the time the files were copied to the hard drive, the public body has implemented changes to the way electronic information is managed. Staff who are required to work overtime either stay on site or use work tablets/laptops through an authorized VPN. Since the break-in, the use of unencrypted hard drives has been prohibited and the public body plans to implement the Digital Integrated Information Management System (DIIMS) by the end of 2023. DIIMS is an electronic information system that allows files to be managed securely throughout their life cycle. It also limits the need for hard drive backups, but for those still required the public body is creating a trackable inventory of hard drives.

[35] In addition, privacy training for employees was made mandatory, and a "clean desk principle" was introduced: paper records are to be locked in desk drawers or cabinets when not in use, and 'convenience copies' of client information are to be securely destroyed at the end of each day.

[36] The public body has reported partial success at implementing these changes. While privacy training is now mandatory, only 69% of the public body's staff had completed it as of September 19, 2023, six months after the breach. Records management training to help staff move to DIIMS was delayed by wildfire evacuations in the summer of 2023 but has now been completed, and a plan to implement DIIMS is underway.

[37] In all, the public body has reacted in an appropriate manner, commensurate with the seriousness of the breach. It must be said that the breach and ensuing investigation has revealed that ECE's offices, at least at this one location, was operating without reasonable security arrangements prior to the breach – despite the clear statutory obligation to have such security measures in place.

**The public body's inattention to information security led to the breach.**

[38] The building itself was physically breached during the break-in. The public body relied on the building entrance doors being secured with an electronic fob system. However, the fob records indicate that the perpetrator was able to open the doors without a fob, indicating a fault in the door, the locking mechanisms, or the fob recording system. The building owner has not been able to verify whether the system was functioning properly at the time, and the door system's software has been updated since the break-in.

[39] While the public body was not the building custodian, it was the custodian of personal information which was being stored in the offices. Inasmuch as ECE relied on the building to provide security, it is apparent that there was insufficient diligence applied to ensuring that the building – and its contents -- was in fact secure from wrongful or forced entry.

[40] Beyond the building's front door, the public body was not able to determine whether the Income Security office door was locked at the time of the break-in. Once inside the building, the intruder accessed the Income Security office, rifled through unlocked desk drawers and cabinets, and stole electronics.

[41] The public body's failure to secure the office areas containing personal information led directly to this breach. All these 'storage areas' – desks, cabinets, offices – were unsecured; ECE appears to have been relying on the front door's security and, perhaps,

a belief that the risk of a break-in was low because it hadn't happened recently in that particular building.

[42] The public body failed to secure paper client files, leaving them in plain view on desks. All file folders were accounted for and ECE reports that no files or information from the files was determined to be missing. However, it is possible that these clients' personal information was viewed or copied. The risk is low, perhaps, but not zero.

[43] Again, the public body's failure to secure its files led directly to the privacy breach. Had the hard drive been properly secured and had the paper files been stored in appropriate locked cabinets the break-in may not have led to a privacy breach at all. It appears that this insecure approach to client privacy was widespread within the office. Any person entering this work area 'after hours' had seemingly unfettered access to large amounts of client personal information in paper and electronic formats. I infer that the housekeeping staff for the office would regularly have had the same access to files as the intruder had at the time of the break-in. In my view, it is fair to describe the situation as systemic inattention to information security throughout this workspace.

[44] The Government of the Northwest Territories' Electronic Information Security Policy reads, in part:

> This Policy provides direction on how the Government of the Northwest Territories (GNWT) will adhere to information security directives, standards, and procedures. This policy also sets out baseline requirements and responsibilities for the secure use of information, information systems, and technologies, in order to fulfill our mandates, support program, and service delivery, achieve strategic priorities and meet accountability obligations prescribed by both legislation referred to in this policy and legislation specific to the departments, boards and authorities.

[45] The accompanying Electronic Information Security Standards describe best practices for secure management of information:

> SM4.4 Physical Protection
>
> (…)
>
> Physical controls should protect:
>
> - (…)
> - Important papers and removable storage media such as CDs, diskettes and tapes against theft or copying (…)
> - Easily portable computers and components against theft, by using physical locks and indelibly marking vulnerable equipment
>
> SM5.4 Remote Access

> Computers to be used by GNWT staff working in remote locations (typically desktop or laptop PCs) must have purchases authorized by the Technology Services Centre, tested prior to use, supported by effective maintenance arrangements, and protected by physical controls.
>
> (…)
>
> Staff working in remote locations, including public areas, such as trains, airports or from home, should be:
>
> - Authorized to work in specified locations
> - Have the skills to perform required security tasks
> - Made aware of the additional risks associated with remote working, including the increased likelihood of theft of equipment or disclosure of confidential information
> - Made aware of approved GNWT enhanced security options
> - Provided with technical support
> - Be in compliance with legal and regulatory requirements
>
> IP2.7 Physical Access
>
> (…)
>
> Physical controls should be provided to protect:
>
> - Important papers and removable storage media (such as CDs and diskettes) by locking them away when not in use, for example in compliance with a "clear desk" policy
> - (…)
> - Easily portable computers and components by using physical locks and indelibly marking vulnerable equipment

[46] Overall, the public body's attention to protecting client privacy fell short of the Act's requirements and short of GNWT's information security policy and standards. Important papers and removable storage media were not locked away. The employee who copied the personal information to the portable hard drive had not been made aware of enhanced security options such as secure VPN access to the network and did not comply with legal and regulatory requirements for securely destroying the duplicate copies of files containing personal information when they were no longer needed.

[47] There was, in my view, a demonstrable lack of reasonable security arrangements, and ECE did not attempt to justify the existing situation; rather, it focused its efforts on

investigating the incident and taking various measures to increase security to prevent any further incidents in the future.

**The public body needs to create a workplace culture oriented to protecting privacy.**

[48] The public body's general approach to protecting privacy prior to the breach did not meet the standard required by the Act. Had this incident not occurred, that approach might still persist today. "Reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal" is the standard. Various physical, technical, and administrative safeguards should be used, individually or in combination, to protect the privacy interest in personal information. Unfortunately, it appears that the only safeguards in place were the main building doors. Once the intruder got past the doors no further measures were in place to protect sensitive personal information held on the portable hard drive or in the paper files left out in plain view.

[49] ECE has recognized that this office required improvements to its information security. It is obvious that the public body needed a shift in workplace culture to prioritize protection of personal information as required by the Act. While several practical steps have been taken, it is concerning that only 69% of the public body's employees had completed mandatory access and privacy training six months after the break-in. This percentage should be much higher.

[50] A good deal of work went into investigating this breach and mitigating its effects that the public body could have put into implementing the technical, administrative, and physical safeguards that should have been in place all along:

a. Locks were available to secure client personal information, but not used.

b. The transitory duplicate records on the hard drive should have been securely destroyed when they were no longer needed for reference instead of being kept in an unlocked drawer for years.

c. Information security directives, standards, and procedures had been developed but were not followed.

[51] The public body has the tools it needs to comply with the Act. It chose not to use them, and this choice resulted in a privacy breach that created a real risk of significant harm to thousands of individuals.

**RECOMMENDATIONS**

[52] Training:

Most privacy protective systems will require employees to receive training in its use. I note with approval that within six weeks of the breach the Department had directed all of its employees to complete the online Information Security Awareness Training program; however, six months after the breach, only 69% of staff at the public body had completed the program. I recommend that the public body take steps to ensure that:

a. all current staff successfully complete privacy training without further delay, and

b. all new staff successfully complete the training program before accessing personal information held by the public body.

c. In regard to the planned implementation of DIIMS, all new and existing employees are provided with appropriate training and possess sufficient skills and knowledge in the use of DIIMS, commensurate with each employee's scope of employment and anticipated use of DIIMS.

[53] Equipment:

I recommend that

a. ECE should ensure that employees only access personal information for work purposes using equipment and software applications issued or approved by the public body. Employees should not use privately owned equipment when accessing personal information for work purposes.

b. If an employee uses the internet to access personal information held by the public body, access should only occur using a virtual private network or other mode of encrypted, secure connection that will prevent unauthorized access by third parties.

c. Unencrypted portable devices should never be used to transport personal information.

d. Client information should be secured in locked cabinets or password-protected electronic systems, with security measures that ensure only those employees who need access to personal information have access to that information.

[54] Records Management:

a. Convenience copies of records containing personal information should be destroyed at the end of the workday or otherwise as directed by the Records Disposition Authority.

Andrew E. Fox
**Information and Privacy Commissioner**