Investigation Report 26-02

Privacy breaches following the Lapu Lapu Day Festival

February 2026

CANLII CITE: 2026 BCIPC 10
QUICKLAW CITE: [2026] B.C.I.P.C.D. No. 10

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

WHO WE ARE

Established in 1993, the Office of the Information and Privacy Commissioner provides independent oversight and enforcement of BC's access and privacy laws, including:

• The *Freedom of Information and Protection of Privacy Act* (FIPPA), which applies to over 2,900 public bodies, including ministries, local governments, schools, crown corporations, hospitals, municipal police forces, and more; and

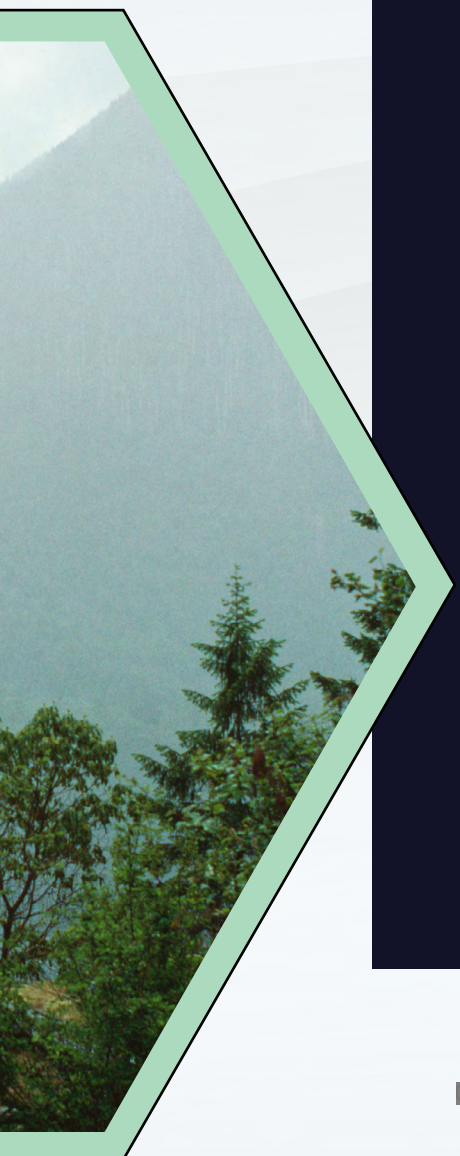
• The *Personal Information Protection Act* (PIPA), which applies to any private sector organization (including businesses, charities, non-profits, and political parties) that collects, uses, and discloses the personal information of individuals in BC. PIPA also applies to any organization operating in BC that collects, uses, or discloses personal information of any individual inside or outside of BC.

Michael Harvey is BC's Information and Privacy Commissioner.

The Office of the Information and Privacy Commissioner for BC respectfully acknowledges that its offices are located on the traditional territories of the lək̓ʷəŋən-speaking people of the Songhees and Esquimalt Nations.

As an Officer of the Legislature, the work of the Commissioner spans across British Columbia, and the OIPC acknowledges the territories of First Nations around BC and is grateful to carry out our work on these lands.

CONTENTS



COMMISSIONER'S MESSAGE

First and foremost, I want to express my sympathy and condolences to all those who experienced the tragedy at the Lapu Lapu Day festival. They have been front of mind for myself and those within the Office of the Information and Privacy Commissioner who worked on the investigation that led to this report throughout the process.

We have taken a trauma-informed approach to this investigation, which included consulting with a clinician as to how to be transparent about what happened, while respecting those directly impacted.

This report does not go into the details of what happened on that day – rather it focuses on what happened soon after, at the health authorities that served those needing care. This report describes how 36 people that worked in health care did not respect the privacy of patients in the aftermath. They violated the privacy of those who had just been through a terrible and life-changing experience. My intention with this investigation was to better understand why and how privacy breaches occurred, and how to better protect patient information from snooping in the future.

A number of factors led to the decision to publish our findings in this report. It is important to be transparent about what happened so we can know and identify any failings in how the health care system protects our personal information – especially in times of crisis.

To that end, I also think it is important to document the accountability that health authorities and their employees have under the *Freedom of Information and Protection of Privacy Act* to protect patient data, including acknowledging steps taken to uphold that accountability. And making the recommendations in this report available to all public bodies enables them to better prevent and respond to snooping - not just for the health authorities discussed, but to all those who have the privilege and responsibility of managing our health care data.

The majority of snooping-related privacy breaches that are reported to my office every year involve the health sector. There are likely several reasons for this, including the large number of people employed in our medical system, the vast amount of sensitive personal information that health care bodies hold on those in British Columbia, and the safeguards that health authorities have in place to detect snooping and report privacy breaches to the OIPC.

These safeguards are increasingly important. As we move deeper into a digitization of healthcare services, where more information is collected and accessible through the use of multiple information systems across health authorities, every health authority and everyone working in the health care system must uphold their obligations to protect personal information. Only in this way will people fully trust their health care providers with their most sensitive information.

Snooping is illegal, unethical, and an egregious and intentional invasion of our privacy. These actions lead to negative outcomes for all involved. It is an affront to our dignity and

autonomy in terms of being able to keep our health information private. It also breaks trust with those in health care that are serving us in a time of need. It could not be simpler: providing care for individuals also means respecting their privacy.

Finally, one of the recommendations in this report is that affected individuals are notified as per the requirement in FIPPA. Two health authorities that reported breaches to the OIPC initially took the position that they were not required to notify and that doing so could cause unnecessary stress on these patients. In effect, they were of the view that it was better that they didn't know; that knowing that their privacy had been invaded would cause further harm through the distress it may cause.

I want to acknowledge that this position was not taken lightly, and came from a place of genuine reflection and concern. However, public bodies need to be careful when making decisions about people's right to know how their own information has been handled by those entrusted with it. People living in British Columbia should be able to know if their sensitive medical information has been breached and how that breach was remedied. This is the only way that individuals affected by a breach can take steps to protect themselves. It also encourages accountability of health care bodies, including taking proactive and preventative measures to protect private health information.

I know that the health authorities take this issue seriously and I would like to acknowledge the steps, including proactive steps, they took to safeguard patient information in what was an unforeseen and unprecedented tragedy.

While the fact that the snooping occurred by so many employees is evidence that safeguards were not perfect, and this report has recommendations for improvement, readers should know that the health authorities all had elaborate regimes in place to prevent, detect, and respond to snooping. It is my hope that the report will further those efforts and thus be of benefit to both the health authorities and those they serve.

Michael Harvey
Information and Privacy Commissioner for British Columbia

EXECUTIVE SUMMARY

Between April 30, 2025 and June 20, 2025 the OIPC received breach notifications from the Vancouver Coastal Health Authority (VCH), the Fraser Health Authority (FHA), Providence Health Care (PHC), and the Provincial Health Services Authority (PHSA) for privacy breaches associated with the tragedy that occurred at the Lapu Lapu Day festival on April 26, 2025. These incidents involved intentional, unauthorized access to patient personal information – often referred to as "snooping"- by employees.

Half of the individuals who received care at medical facilities following the tragedy subsequently had their privacy breached. In total, 71 snooping incidents on the medical records of 16 individuals were reported.

These breaches were committed by 35 employees of the health authorities and PHC, and in one other case, by an assistant at a physician's office who had access to an FHA electronic medical records system. In most cases, these employees invaded individuals' privacy to satisfy their own curiosity.

This report sets out the OIPC investigation into these breaches. The Commissioner found that the breaches committed at the health authorities violated s. 25.1 of the *Freedom of Information and Protection of Privacy Act* (FIPPA). This section prohibits an employee, officer or director of a public body or an employee or associate of a service provider from collecting, using or disclosing personal information except as authorized by FIPPA.

The employees who were caught snooping were all disciplined by their employers. This discipline varied from letters of expectation to terminations, with the majority of cases resulting in a suspension. In addition, some employees had their actions reported to their respective regulatory college.

The Commissioner also examined whether the health authorities had reasonable safeguards in place to prevent snooping. He found that, despite the breaches that took place, the health authorities had the expected safeguards in place and are working to strengthen them.

The report also documents how the health authorities and PHC quickly realized the potential for snooping in the aftermath of the tragedy. Some of the actions they undertook, either alone or in concert, were: to send notices reminding staff about the need to respect privacy and confidentiality in high profile incidents; suspending access to records where possible; flagging and appending additional warnings on the medical records of those admitted to their facilities if their names were publicly known; proactively auditing access to those individuals' records; reporting suspected instances of unauthorized access to the OIPC; and investigating potential contraventions and imposing consequences.

Fraser Health notified two individuals and a representative of a deceased individual that their privacy had been breached and conveyed the steps that were being taken to prevent any further harms. Vancouver Coastal Health and PHSA, after assessing the risk of harm to individuals whose privacy was violated, initially took the position that notification was not required and could itself result in further harm.

However, for the reasons given in the report, the OIPC concluded that the health authorities had a legal obligation to notify as required by FIPPA, and this obligation has since been met.

The report includes five findings regarding FIPPA compliance and nine recommendations for strengthening safeguards to prevent snooping. The health authorities have accepted the recommendations, and the OIPC will follow up on their progress.

A summary of recommendations can be found on page 44.

BACKGROUND

On April 26, 2025, the Filipino-Canadian community celebrated Lapu Lapu Day in Vancouver, British Columbia. The end of the festival was marred by tragedy when the driver of an SUV drove through the crowd, killing 11 people and injuring dozens of others. Thirty-two people, including deceased individuals, were sent to hospitals and facilities operated by the Vancouver Coastal Health Authority (VCH), the Fraser Health Authority (FHA), Providence Health Care (PHC), and the Provincial Heath Services Authority (PHSA). Half of those sent to medical facilities would have their privacy breached shortly thereafter.

On April 30, 2025, VCH reported the first breach of patient information to the Office of the Information and Privacy Commissioner (OIPC). At that time, the health authority reported one instance of suspected unauthorized access to patient information. They also said that they were taking steps to restrict access to identified patient records and auditing their electronic medical records system to identify and respond to any other cases of unauthorized access.

The OIPC received further breach reports from FHA and PHSA on May 30, 2025. On June 20, 2025, PHC also reported a related breach to the OIPC.[1]

The breaches involved individuals with access to health care systems using that access in an unauthorized manner to view the personal information of patients – an act commonly referred to as "snooping."

1 A timeline of key events is in Appendix A

METHODOLOGY

This investigation was conducted under section 42 of the *Freedom of Information and Protection of Privacy Act* (FIPPA) pursuant to the Commissioner's power to conduct investigations to ensure compliance with the Act, as well as the Commissioner's general responsibility for monitoring how FIPPA is administered.

The breach reports were originally assigned to OIPC investigators for monitoring the health authorities' breach response to ensure that the response complied with the health authorities' obligations under FIPPA. However, given the seriousness of this matter, including its breadth and effect on privacy and trust in the healthcare system, the Commissioner decided to investigate what occurred across the health authorities that reported snooping activities.

The OIPC issued a notice of the investigation to the health authorities on June 19, 2025. Two weeks later, on July 03, 2025, the OIPC issued a revised notice to the parties, as a result of PHC also reporting a breach to the OIPC.

The OIPC sent a series of questions to the three health authorities and PHC. As OIPC investigators had reviewed the breach reports from each of the respective health authorities on an individual basis, the questions in the investigation across the health authorities were built on information already provided to the OIPC.

The OIPC sent several rounds of follow-up questions to each health authority and met with them to ask further questions and clarify any matters material to the investigation. The information gathered included:

- the dates and location of unauthorized access by specific employees;
- the systems and types of patient personal information accessed;
- the reasons provided by the employee for accessing the personal information; and
- the consequences that followed.

Information also included answers and documentation responding to OIPC questions about each of the issues discussed below, including:

- the safeguards the health authorities have in place to prevent snooping;
- the steps they took to identify and contain the breaches;
- their assessment of possible harms;
- their actions and views with respect to notification; and
- information related to how similar incidents can be prevented going forward.

The health authorities and PHC cooperated fully throughout the investigation.

Issues for investigation

The issues in this investigation address whether the health authorities and their employees acted accountably under ss. 25.1, 30 and 36.3 of FIPPA. These provisions are set out in full in Appendix B.

Section 25.1 is a general prohibition on the collection, use, and disclosure of personal information by an employee, officer or director of a public body or an employee or associate of a service provider. This prohibition applies unless the activities relating to personal information are authorized by another provision in FIPPA. In this case, the activity in question required a 'use authority' under s. 32. The issue under s. 25.1 is:

> *1. Was personal information improperly accessed?*

Under s. 30 of FIPPA, the health authorities must establish reasonable safeguards to protect against the unauthorized use of personal information. The issues under s. 30 are:

> *2. Did the health authorities have reasonable safeguards in place to prevent unauthorized access to personal information?*

> *3. Did the health authorities take reasonable steps to respond to the privacy breaches?*

Finally, under s. 36.3 of FIPPA, public bodies, including health authorities, must notify individuals and report the matter to the OIPC without unreasonable delay when a breach could reasonably be expected to result in significant harm. The issue under s. 36.3 is:

> *4. Did the health authorities' response to the alleged breaches comply with their obligations, if any?*

PRELIMINARY MATTER

Health authorities, PHC, and accountability under FIPPA

The health authorities subject to this investigation are VCH, FHA and PHSA (collectively, the "health authorities"). Each of the health authorities is a public body under FIPPA,[2] and they all reported privacy breaches to the OIPC following the tragedy at the Lapu Lapu Day festival.[3] As public bodies, the health authorities are responsible for managing personal health information consistent with their responsibilities under FIPPA, including carrying out lawful collection, use and disclosure of personal information, securing personal information, and responding to privacy breaches.

The breaches reported to the OIPC occurred at sites across each of the health authorities. While some of those sites are hospitals and distinct entities that are considered public bodies under FIPPA,[4] health authorities are also public bodies under FIPPA with hospitals falling under their responsibility. In this investigation, it was the health authorities that provide and manage the systems that were compromised and under FIPPA are responsible for safeguarding patient data in those systems.

In addition to the health authorities, PHC reported a related privacy breach to the OIPC. PHC is a non-profit organization that operates hospitals and health care services in the Lower Mainland. As an organization, PHC is generally subject to the *Personal Information Protection Act*.[5] However, PHC operates a department named Health Information Management (HIM), which provides services to each of the health authorities under a Master Services Agreement (MSA).[6] These services primarily include patient registration, records management, transcription and coding.[7] The MSA includes a Service Schedule about Health Information Management that explicitly directs HIM "to perform duties and exercise functions of the Customer Organization [i.e. the health authorities] under FIPPA."[8] Further, it is PHSA that oversees the HIM program even though HIM employees are employed by PHC.

---

2 VCH and FHA are health authorities established under section 4(1) of the *Health Authorities Act* (regional health boards are commonly referred-to as health authorities in BC), and they are each a "public body" as defined under FIPPA as they are each a "health care body" and a type of "local public body". PHSA is specifically designated as a "public body" under Schedule 2 of FIPPA.

3 First Nations Health Authority, Interior Health Authority, Island Health Authority and Northern Health Authority did not report any related breaches to the OIPC, and OIPC investigators confirmed directly with each of them that they did not experience any breaches related to the tragedy.

4 The Schedule 1 definition of "public body" under FIPPA includes "hospitals as defined in section 1 of the *Hospital Act"*, because it includes a "local public body" which includes a "health care body" which in turn includes hospitals. An institution becomes a "hospital" under the *Hospital Act* when it is designed by the Minister (for example see Ministerial Order 352/2011).

5 Decision F09-05, December 16, 2009, available online at: https://www.oipc.bc.ca/documents/decisions/138.

6 The MSA was established in January 2011 and is between PHSA (including various province-wide entities), FHA, VCH, and PHC.

7 Appendix 1 of Schedule 2J of the MSA.

8 Para. 2.1 of Schedule 2J of the MSA.

During the investigation, the OIPC sought to clarify the lines of accountability under FIPPA when it came to the provision of services by HIM to health authorities, as PHC reported a breach to the OIPC. Based on discussions with legal counsel from PHC and PHSA, a review of contractual material, and information from PHSA's general counsel,[9] the OIPC concluded that a privacy breach caused by a HIM employee is the responsibility of the health authority which has its data compromised.

Under FIPPA, public bodies are responsible for services delivered by a service provider.[10] As a result, when PHC is providing HIM services to a health authority, it is the health authority that PHC is providing services to that is responsible for those services under FIPPA. The accountability of the health authority also has practical application—it is the health authorities that have the relationship with patients and are in the best position to address a breach, including issuing notification when needed or appropriate.

A service provider relationship applies to what occurred in the one HIM breach at issue in this report. The breach occurred at a VCH hospital. It was detected by VCH, who reported it to their service provider (PHC). PHC investigated and determined that a breach had in fact occurred, reported the breach to the OIPC, and disciplined their employee. Nonetheless, VCH is responsible for addressing the breach, and had PHC not reported it to the OIPC, then VCH would have had the ultimate accountability under FIPPA to do so.

The responsibilities that public bodies have under FIPPA for the actions of the service providers they engage protects the people of BC from gaps in accountability when privacy incidents occur. This is broadly reflected in FIPPA's general purpose, "to make public bodies more accountable to the public and to protect personal privacy".[11] Clarity on lines of accountability is critical to any public body engaging an effective breach response. As the Province moves towards a new health information framework, government must ensure that all health organizations that provide care to British Columbians are accountable for the personal information of those they serve, including when they engage service providers to offer those services.

9 October 3, 2025 letter from PHSA General Counsel to OIPC Director of Investigations.

10 Section 3(2)(b) of FIPPA provides that Part 3 of FIPPA applies to employees of a service provider, which is defined as a person (including incorporated Societies, such as Providence) retained under a contract to perform services for a public body.

11 Section 2(1) of FIPPA.

DISCUSSION

The unauthorized use of personal information by employees of a public body is commonly referred to as ‘snooping.’ This occurs when an employee accesses personal information that they do not need to perform their duties. In a health care setting, it often means accessing medical records when the employee is not actively involved in providing care or other work in support of that care.

Snooping is the act of intentionally accessing personal information without authorization. It is particularly egregious in health care due to the sensitivity of personal information involved and the relationship between patients and health care providers. The idea that our personal information may be accessed and used by others for reasons unrelated to the provision of care can be incredibly harmful.

For patients, having their personal privacy violated in this way can lead to further stress at a time when their focus should be on recovery. For both patients and the public, it can compromise trust in our health care system and its ability to protect our personal information.

The reputational damage to our health care system that follows can reduce our willingness to share personal information with health care providers, which can ultimately compromise care. In the digital age, with personal health information stored in information systems and accessed in seconds by way of a login, it is of paramount importance that public bodies have measures in place to secure personal information from unauthorized access.

Issue 1: Was personal information improperly accessed?

FIPPA provides that an employee, officer or director of a public body or an employee or associate of a service provider must not collect, use, or disclose personal information except as authorized by FIPPA.[12]

In total, the health authorities and PHC identified 71 instances of unauthorized access to patient records. Depending on the incident, amongst the information accessed without authorization was patient demographic and contact information (e.g. names, date of birth, address, and health care numbers), and medical history (e.g. diagnosis, medications, lab results, case notes and summaries).

FIPPA defines "personal information" as "recorded information about an identifiable individual other than contact information."[13] The latter refers to information that enables an individual at a place of business to be contacted and is not at issue here (in other words, in the context of a patient receiving health care, their personal contact information is "personal information").

I find that the breached information constitutes "personal information."

The health authorities have this information to provide health care, and the ability to access that information in a timely manner is part of the provision of that care. However, access to medical information should be limited to those that need it to deliver healthcare services.

Each health authority undertook a process for determining whether an employee's access to patient medical records was necessary. This involved the privacy office reviewing audit logs, consulting with employees' supervisors to confirm whether the access was part of those individuals' duties, interviews with employees, and the involvement of human resources.

The systems that were breached required employees to log in and their activity was recorded and audited. The results of those audits were investigated by the health authorities and PHC and were determined to constitute snooping. In only one case did an employee deny accessing the files at issue.

The health authorities and PHC ultimately determined that 36 individuals inappropriately accessed patient records, one of which is an employee of PHC, and the other a medical assistant at a physician's office who had access to FHA's Meditech system.

12 FIPPA at s. 25.1

13 Schedule 1 of FIPPA. "Contact information" in this definition refers to information that enables an individual at a place of business to be contacted. It is not at issue in this investigation; in the context of a patient receiving health care, their contact information is personal information.

In some cases, employees accessed patient records multiple times. For example, in one instance, an employee accessed the personal information of nine patients in a single day; in another case, an employee repeatedly accessed one patient's file.

Moreover, two employees went on to disclose patient information to colleagues.

The health authorities heard a variety of reasons for accessing patient records. These reasons were investigated by the health authorities and determined to be unauthorized under FIPPA.

The OIPC consolidated the stated reasons across the health authorities that reported breaches. They included personal, work, or other reasons, and are summarized in Table 1. In some cases, more than one reason was given.

Table 1: Reason(s) provided for accessing personal information			
Alleged reason(s) for each instance of access[14]	**PHSA**	**FHA**	**VCH**
Personal reasons			
Curiosity	31	2	3
Personal concerns (about individuals who experienced the tragedy)such as determining risk/ability to provide care or emotional/mental preparation to provide care	8	1	0
Emotional distress	1	1	0
Concerns for their community	5	0	1
Employee grieving the loss of a friend[15]	0	1	0
Work reasons			
To complete a task on a future date	1	0	0
Directed by supervisor	1	0	0
Delegated with the task	1	0	0
Educational purposes	1	0	0
Belief that access was related to work responsibilities	3	0	0
Other			
Denied accessing records	3	0	0
Reason that could not be determined as the employee could not be interviewed	0	1	0
Employee was asked by family member/friend of an affected individual to access records	0	1	0

14 As provided by the health authorities and and determined to be unauthorized under FIPPA.

15 Note: the friend has no connection to the Lapu Lapu tragedy

The employees that accessed the personal information occupy a range of positions across health authorities, as summarized in Table 2.[16]

Table 2: Employees who accessed personal information			
Position	**PHSA**	**FHA**	**VCH**
Administrative support worker	10	2	1
Assisted living worker	0	1	0
Nurse*	11	2	2
Nursing aide	0	1	0
Office assistant	0	1	0
Clinical assistant	1	0	0
Clinical fellow*	1	0	0
Medical student*	1	0	1
Patient liaison	1	0	0
Pharmacist*	1	0	0
TOTAL	**26**	**7**	**4**

** These positions are subject to regulatory colleges.*

Each of the health authorities and PHC determined, through a process that included audits, checking with supervisors and interviews with employees, that access in these cases constituted privacy breaches. The steps taken by the health authorities and PHC aligns with the responsibility on public bodies to manage privacy requirements, including breaches, and to investigate and levy discipline as appropriate when contraventions occur. As the oversight body, the OIPC may monitor and investigate that work, and where appropriate make findings about what occurred and the application of FIPPA.

The authorities under FIPPA that a public body, including its employees and service providers,

16 One of the individuals below accessed the personal information of affected individuals in more than one health authority and is therefore counted twice in the table.

can rely on to use personal information are limited.[17] They include:

- for the purpose for which the information was obtained or compiled, or for a use consistent with that purpose;
- for a purpose for which the individual consents to the use of their information; or
- for a purpose for which the information may be disclosed to the public body under s. 33.

None of these purposes apply in the cases where a breach occurred. While the information accessed was obtained or compiled for the provision of medical care, the health authorities and PHC determined that the use of the patient data did not accord to that purpose – even in cases where the employee claimed to have a legitimate need to access the patient records.

Further, no evidence or information has been provided that gives reason to believe that patients in question consented to health authority employees accessing their records, whether for curiosity or any of the other reasons given by the employees who snooped. In addition, there is nothing in the material the OIPC reviewed to indicate that the information accessed was both provided by another public body under s. 33 and accessed for the purpose of that provision.

Finding 1

Each of the cases reported by the health authorities and PHC represents a contravention of s. 25.1 of FIPPA.[18]

17 See s. 32 of FIPPA.

18 This finding does not include a physician's assistant who inappropriately accessed FHA's Meditech system, as they are not an employee of a health authority or a service provider to one. Such access likely contravened the *Personal Information Protection Act*, and FHA followed up with the physician assistant's employer and revoked their access to FHA's systems.

REASONABLE SAFEGUARDS

Issue 2: Did the health authorities have reasonable safeguards in place to prevent unauthorized access to personal information?

Under s. 30 of FIPPA, public bodies must have reasonable safeguards in place to prevent the unauthorized collection, use, disclosure, or disposal of personal information.

Reasonableness does not mean perfection, but it may require a high level of rigor depending on the situation.[19] In this case, the medical information of patients is highly sensitive and the relationship between patients and the health authorities is based on trust and dependency. These criteria alone are enough, in my view, to indicate that health authorities must deploy significant and robust safeguards to prevent snooping.

The safeguards that should be deployed in the context of preventing unauthorized access to medical records have been addressed in reports and guidance documents from privacy commissioners across the country, including from this office.[20] These materials refer to a number of administrative, technical, and physical measures.

The discussion and findings that follow consider whether the health authorities had reasonable safeguards in place to guard against employee snooping, rather than the overall security of any one program or system.

19 Office of the Information and Privacy Commissioner for BC. Investigation report F06-01: *Sale of Provincial Government Computer Tapes Containing Personal Information.*

20 Information and Privacy Commissioner of Ontario. *Detecting and Deterring Unauthorized Access to Personal Health Information*. Office of the Information and Privacy Commissioner for BC. Audit & Compliance Report F15-02: *Examination of British Columbia Health Authority Privacy Breach Management*. Office of the Information and Privacy Commissioner for BC. Investigation Report F10-02: *Review of the Electronic Health Information System at Vancouver Coastal Health Authority Known as the Primary Access Regional Information System* ("Paris"). Office of the Privacy Commissioner of Canada. *Ten Tips for Addressing Employee Snooping.*

Administrative Safeguards

Administrative safeguards help employees understand, value and commit to their legal and professional obligations to protect privacy.

These safeguards must include procedures for deterring and responding to unauthorized access to personal information, including consequences for employees who engage in such conduct. In this way, administrative safeguards protect patients and public bodies. They also educate employees about what actions could threaten employment.[21]

Training and awareness

Training is necessary for employees to understand the need for privacy and confidentiality, their legal and professional obligations, the processes put in place to protect privacy, and consequences for failing to adhere those requirements.

Each health authority confirmed that they deliver mandatory privacy training, which must be taken every one or two years. The training delivered to employees includes information about snooping and its consequences.

All but one of the employees who snooped worked for the health authorities or a service provider and completed mandatory privacy training before they engaged in snooping.[22]

Recommendation 1

Clearly convey through privacy training that system activities are monitored and that discipline will be imposed for snooping.

21 Employees should be well aware that snooping violates both their legal and professional obligations. These obligations are made clear through privacy training; written documents, such as standards of conduct, confidentiality agreements and privacy policies; and notices appended to patient records. The obligations on employees to protect privacy and confidentiality also include professional standards, such as those found in the BC College of Nurses and Midwives Privacy and Confidentiality Practice Standard, and the Canadian Medical Association's Code of Ethics and Professionalism.

22 The other individual worked as a Medical Office Assistant for a doctor's office and had access to FHA patient data through their external access program. They have since had their access revoked to all FHA systems.

Privacy policies

Having a privacy policy is both a required part of a privacy management program and a key part of reasonable security safeguards. The policy should make clear to public body employees what the rules and expectations are for handling personal information and how they work in practice. This includes potential consequences for when those rules are breached.

The OIPC reviewed the health authorities' privacy policies and procedures. These policies set out legal and professional requirements for handling personal information. They also set out how the health authority - including its employees - will meet the privacy requirements in FIPPA.

Each of the health authorities' privacy policies say that employees are granted access to personal information on a 'need-to-know' basis to perform their duties. They also provide further explanations as to when and how personal information can be accessed and used (e.g. when a patient consents to that use).

If employees are unsure about whether they have authority to access and use patient data, the policies identify who they should contact. These policies also include information about the consequences for failing to abide by them, such as the loss of employment or medical privileges. In addition, the health authorities require employees to read and be familiar with their privacy policy.

Confidentiality agreements

Confidentiality agreements or undertakings require employees to commit - in writing - to their privacy and confidentiality obligations. These agreements make those obligations clear and are important for holding employees accountable for their actions.

The health authorities all use confidentiality agreements. They are concise documents that employees are required to sign as part of the onboarding process, including by the employees found to have snooped on patient records.

The documents vary somewhat, but all say that access to personal information can only occur in respect of required job duties and refer to more detailed privacy policies.

Two of the three agreements refer to consequences for non-compliance and one of them refers to the fact that system use is monitored and recorded, and that compliance audits are conducted.

Recommendation 2

Plainly state in confidentiality agreements that system use is monitored and consequences will be imposed for breaches of privacy and confidentiality.

Privacy notices

Privacy notices and flags remind employees that the personal information in a system can only be viewed for a legitimate purpose. They also can require employees to confirm a patient care or other legitimate relationship with a patient *before* accessing their records.

Most of the systems at issue here use these kinds of notices. For example, the Cerner system, used by VCH, PHSA, and PHC, has a just-in-time declaration that requires employees to confirm a clinical or other legitimate relationship with a patient before accessing their records.

Other notices reviewed by the OIPC, such as the ones used in CareConnect, Meditech, and PACS also require that the user affirm a relationship with the patient, with the latter two stating that access to a patient file is recorded.

FHA's UCI and Paris systems also appends a notice to patient files, but unlike in Cerner, employees do not have to click on it to access the underlying records.

Once FHA identified patients who experienced the tragedy, they flagged their records in the Meditech system and appended notices that said that any access to those files is confidential. Employees were required to accept the notice, and no unauthorized access occurred after the notices were added.

Privacy notices are important as they offer a point-in-time reminder about patient privacy. However, it is difficult to gauge their overall efficacy in this case as a number of employees accepted a privacy notice before proceeding to snoop on records (i.e. they falsely affirmed a legitimate need to access patient records). Conversely, FHA found that notices were effective once placed on files, and they likely deterred additional employees from clicking through to the records at VCH and PHSA.

The routine nature of privacy notices does not absolve employees from their responsibility to read them and honestly affirm whether they have a legitimate need to view patient records, which is a matter that can be explicitly addressed in training. Privacy notices are also valuable to health authorities for holding employees to account, as the health authority can show that the employee claimed to have a need to view records when in some cases they did not.

Recommendation 3

The health authorities revisit their privacy notices. For Fraser Health this includes making greater use of Meditech privacy notices and working to implement a comprehensive confidentiality warning in its Paris system.

End-user agreements

End-user agreements explain and commit users to the terms and conditions of electronic records systems, including privacy requirements. This can help users understand and agree to conditions prior to being granted access to a system containing electronic health records.

Most of the systems considered in this report have end-user or terms of service agreements that employees must read and agree to before being granted access. For example, Cerner, which is used by VCH, PHSA and PHC, requires employees to attest that they will only access information in the system as authorized by FIPPA. The notice also states that failing to abide by the terms of use may lead to disciplinary action, including revoking access privileges, professional sanctions, suspension or termination of employment.

PHSA also explained that its terms of use for clinical systems includes information about the consequences of system misuse and requires employees to acknowledge and accept confidentiality rules. They also noted that the end-user agreement for CareConnect, which provides for broad inter-jurisdictional access to patient data, plainly notes that access to the system is audited, unauthorized use will be investigated and disciplinary consequences imposed.

FHA said that users do not sign end-user agreements for each system but instead are required to acknowledge policies and agreements at onboarding, including the privacy policy, confidentiality agreement, and standards of conduct.

End-user agreements, along with the other documents described above, are part of a multi-faceted approach to conveying privacy responsibilities to employees and the consequences for not abiding by them. While FHA should consider adding this protective measure, the fact that it does not leverage end-user agreements is alone not enough to conclude that they do not have reasonable administrative safeguards in terms of employees understanding and committing to their privacy obligations.

Breach management

An established breach management process enables public bodies to respond more effectively to the theft or loss, or the unauthorized collection, use or disclosure of personal information. This is critical to safeguarding patient data in terms of the timeliness and efficacy of the breach response.

The OIPC reviewed the health authorities' privacy breach response procedures. These documents address the responsibilities of employees and the steps that need to be taken in response to an actual or suspected privacy breach. Having documented breach response procedures helps public bodies address breaches in a consistent and effective manner. In addition to setting out responsibilities for employees, the procedure documents also caution that failure to abide by them can result in disciplinary action.

All the health authorities' procedures address the key steps and accountabilities for responding to breaches, however, only PHSA refers to the 2021 amendments to FIPPA that define breaches and mandate privacy breach notification and reporting. The OIPC recommends updating documents where this information is missing, as the amendments added notification requirements and timelines for responding to breaches that could reasonably be expected to result in significant harm.

Recommendation 4

VCH and FHA update their privacy breach procedures to include information about mandatory breach notification requirements.

Discipline

To deter snooping, the OIPC expects health authorities to convey to employees that their system use is monitored, and they will be disciplined for contravening privacy rules.

Each of the heath authorities make this information known to employees through some or all of the documents and processes set out above. In addition, both FHA and PHSA have internal guidance documents that set out disciplinary standards for breaching privacy and confidentiality. The discipline for snooping ranges from written warnings to termination. These documents help the health authorities to apply consistent discipline for privacy infractions. VCH should create a similar document.

Recommendation 5

VCH develop disciplinary guidelines for privacy breaches that involve snooping.

Technical safeguards

The OIPC expects public bodies to have technical safeguards in place to prevent snooping. These include measures that restrict access to personal information and allow the health authorities to monitor and audit system use.

A number of databases were inappropriately accessed in these breaches, which reflects the digital nature of health care information and services, and the need for security safeguards across digital ecosystems to prevent misuse.

Role-based access

Health authorities must implement role-based access to meet the legal requirement in s. 30 of FIPPA.[23]

Role-based access is based on 'need to know' and 'least privilege' privacy principles. Employees are only given access to the type and amount of personal information that they need to

23 OIPC. Audit & Compliance Report F15-02: *Examination of British Columbia Health Authority Privacy Breach Management*. https://www.oipc.bc.ca/documents/audit-reports/2009

perform their duties. In other words, the systems that employees can access, and the personal information that they can retrieve within those systems, is limited to their assigned roles.

All the health authorities use role-based access to limit access to patient data. In addition to role-based access, the health authorities explained to OIPC investigators that in some cases, access to health care records is limited to those working specific programs areas or work sites.

Health authorities employ a large number of people and need to have a process in place for granting and revoking access to information. The Information and Security Policy for VCH, PHSA and PHC includes requirements for registration and de-registration of role-based access to systems and confidential information, including identity assurance procedures. The Policy further stipulates that user access rights must be reviewed at regular intervals. These measures protect against access by those who ought not to have it at all.

Even with processes to keep role-based access up to date, many employees may have access to a specific patient's records at any one time. This can be the case within a hospital or region, or even across regions and organizations. This is especially the case for shared systems used by more than one health authority or other health organizations. While such systems are designed to support integrated multidisciplinary care, they also increase the risk of snooping. This is why health authorities must implement multiple security measures, and at times work together, to protect patient data.

System use is logged, monitored and audited

Logging, monitoring and auditing the use of records systems is critical for security and privacy. In addition to deterring inappropriate use of personal information, these measures enable public bodies to detect and respond to snooping and other threats to data.

The actions users take in electronic medical records (EMR) systems are logged. These systems record who accessed patient records, when and where the access occurred, and the actions that took place (e.g. viewing, modifying, printing, etc.).

The OIPC confirmed that the health authorities conduct proactive and reactive audits to detect anomalous access to patient files. They do this through both regularly scheduled audits and more targeted audits of specific patient files that have been flagged in their systems. Once the health authorities learned the names of those involved, it was through targeted audits of access to their records that the breaches in this investigation were identified.

All the health authorities also noted that they are in the process of implementing new auditing software that will provide for a more automated process for identifying potential misuse of patient data in clinical systems.

Based on the above, the OIPC is satisfied that the health authorities have systems and processes to audit access to medical records.

Physical safeguards

Reasonable security safeguards include physical measures to protect personal information. In the matter at issue here, unauthorized access to personal information occurred through electronic and not physical files. Nonetheless, the health authorities referred to several types of physical security, including those meant to protect digital data, such as restricting access to servers and ensuring that workstations are locked and out of public view. Ultimately, there is nothing in these incidents that suggests that inadequate physical security contributed to unauthorized access to patient records.

Reasonable safeguards to prevent snooping

The discussion above outlines the kinds of safeguards that we would expect for the health authorities to comply with s. 30 to prevent breaches. Administrative safeguards foster a culture of privacy and respect for patient data in the health care system. This includes training and written commitments that employees understand those values and will abide by them. There are also technical safeguards that limit, track and audit what employees can do in electronic medical records systems. In terms of physical security, there is again nothing to suggest that a lack of physical security contributed to these breaches. While certain processes may be improved, especially as it pertains to identifying and responding to breaches, the health authorities have put in place the essential pillars for protecting patient data from snooping.

Finding 2

VCH, PHSA, and FHA employed reasonable security safeguards to protect against unauthorized access to personal information in the context of employee snooping.

BREACH RESPONSE

The OIPC has set out four steps for responding to privacy breaches in a manner that is consistent with the requirement in s. 30 to take reasonable measures to secure personal information. The OIPC considers each step in determining whether a public body's response to a breach met their duty to safeguard personal information. These steps include containment, risk assessment, notification (if required) and prevention.

Furthermore, as a result of an amendment to FIPPA effective February 1, 2023, s. 36.3 requires public bodies to notify affected individuals and the OIPC in specific circumstances when a privacy breach has occurred. This section of the report examines both the overall breach response and the obligation to notify under s. 36.3.

Issue 3: Did the health authorities take reasonable steps to respond to the privacy breaches?

Containment

The purpose of containment is to limit any further unauthorized access to personal information. This can include measures such as locking down access to records or retrieving lost or stolen information.

In response to potential and suspected breaches, the health authorities undertook similar, and at times coordinated, actions.

In anticipation of the potential for snooping, VCH, FHA, and PHC flagged patient records as the names of individuals who experienced the tragedy became known—either by noting those individuals as they were admitted to hospital or upon learning their names through media reports. This enabled them to audit access to those records in the days and weeks following the tragedy.

The PHSA privacy office was first alerted to suspected unauthorized access by VCH, and by other organizations within PHSA. VCH also reported possible breaches to PHC, as they involved HIM employees working at VCH locations.

The health authorities and PHC sent out reminders to employees about patient confidentiality in high profile events. On April 28, two days after the incident, a memo was sent from the VCH Risk Management team that provided privacy and confidentiality reminders that were communicated to employees. On April 30, PHC issued a memo to Program Directors and Physician Program Directors in Saint Paul's Hospital Emergency and Internal Medicine about

patient privacy and confidentiality obligations. And on May 1, a similar notice was sent from the health authorities and PHC to all HIM employees.

In some cases, it was possible to fully restrict access to the records of specific patients, and where this occurred there were no reported breaches. However, fully restricting access to medical records can adversely impact patient care—especially in critical situations. This means that in some cases, patient files were flagged for auditing, or appended with a privacy warning, but were not locked down from access.

The health authorities audited access to the flagged patient files. These audits were conducted for different periods of time, ranging from a week to a month after the incident, and with varying frequency, from daily to weekly reviews.

The audits generated a list of people who accessed the patient files and some of the actions they performed (e.g. view, modify, print, etc.). The privacy offices reviewed the audit logs to determine whether the individual should have accessed the patient record. This determination could be based on several factors, such as shift patterns, site locations, comparison of regular access to records by the employee, and whether they were part of the care team or otherwise supported that specific patient's care.

When the privacy office could not determine whether the access was authorized, they directed the matter to the employee's supervisors who were asked whether the access was necessary for the employee's duties. The health authorities also engaged human resources in their investigations as needed.

Employees were given the opportunity to explain why they accessed one or more of the flagged patient files. They were also asked about any additional actions they may have taken in respect of the compromised information. Where it was confirmed that the employee further disclosed personal information to other employees, the health authority met with those other employees to reassert their privacy and confidentiality obligations.

As a result of these investigations, a variety of sanctions were imposed by the health authorities and PHC, including written reprimands, decommissioning access to records systems, suspensions, and termination. Some employees were also required to retake privacy training and re-sign confidentiality agreements, and all are subject to additional monitoring.

The health authorities made concrete efforts to contain these breaches. They quickly realized that a public tragedy of this nature could result in snooping. They took steps to prevent that from occurring by issuing reminders about privacy and confidentiality, restricting access to certain records, and applying privacy warnings. They also audited access to patient files so they could identify and respond to any breaches that did occur.

The health authorities were not as swift in confirming whether the access to records was in fact unauthorized. Many people treated these patients, and where access appeared to be unnecessary the health authorities took several steps, including interviewing employees about their reasons for accessing the records. This process could take a significant period of time, as some breaches were only confirmed months after the fact. These delays can impede containment efforts as the scope of what occurred was unknown, including whether employees undertook any subsequent actions with patients' personal information that posed additional risks. It is also the case that suspension of their access to patient records or other limits may not be imposed until it is is known whether that access has in fact been abused.

However, I also recognize that these were unforeseen and exceptional circumstances which involved many individuals, both in terms of affected individuals and those who accessed their records. I also recognize that due diligence is required to confirm these incidents, especially as they all resulted in some form of employee discipline (or resignation). Nonetheless, I am of the view that while the overall containment efforts were reasonable, it is in the interest of all parties that the investigations are more timely and that resources should be reallocated to them when needed.

Risk assessment

A public body must assess the risk of harm associated with a breach to determine what other immediate steps are necessary (in addition to containment) and what (if any) notification should or must occur. There are four overarching factors that may be relevant in assessing risk of harms.[24] These factors include:

- the sensitivity of personal information;
- the cause and extent of the privacy breach;
- the individuals or others affected; and
- foreseeable harms.

The health authorities explained their assessment of the harms associated with these breaches. FHA and PHSA identified several potential harms in their initial breach reports to the OIPC. These harms included a breach of contractual obligations, damage to reputation and relationships, failure to meet professional or certification standards, humiliation, identity theft, and mental health stress. While these harms may have been identified as possibilities during the early stages of their breach response, they remain relevant, and some of them, particularly stress and humiliation, continued to be cited in later stages of this investigation.

24 https://www.oipc.bc.ca/documents/guidance-documents/2584

The health authorities also noted that while the breaches were the result of serious employee misconduct, they were contained and there was no evidence of any malicious intent. Other mitigating factors were also cited, particularly by PHSA, who conducted a comprehensive risk assessment. These factors included the fact that the information accessed may not have included stigmatizing medical information, some patient injuries have already been publicly reported, and there was no evidence that those affected by the breach were likely to experience harms as a result.

In considering the four risk factors noted above, there are several circumstances we consider relevant. It remains the case that the breaches involved highly sensitive personal information. They were caused by employees intentionally violating their legal and professional obligations, largely for the sake of curiosity. While these are not necessarily malicious intentions, their intentional and reckless nature indicate a risk that the personal information could be further disclosed due to general curiosity and ongoing public interest in this event. In fact, such further disclosure by employees who snooped occurred in two confirmed instances.

I find that when considered together, the four risk factors indicate that there is a meaningful risk of harm to those whose privacy was breached.

Issue 4: Did the heath authorities' response to the alleged breaches comply with their obligations, if any?

Notification

The results of the above risk assessment led us to conclude that notice to those who experienced the tragedy and whose personal information was breached is warranted. However, this did not occur in most cases, which leads to the question of whether that notice is required under FIPPA.

Section 36.3 requires public bodies to notify an individual and report to the Commissioner when a breach could reasonably be expected to result in significant harm to the affected individual. This provision contains a non-exhaustive list of specific significant harms that trigger the obligation to notify. When this threshold is met, public bodies must carry out notification without unreasonable delay.

Section 36.3(3) sets out two circumstances when a public body is not required to notify affected individuals, even when the obligation to notify is triggered under s. 36.3(2). This includes situations where the notice can be reasonably expected to result in immediate and grave harm to the affected individual's safety or physical or mental health, or if the notice can reasonably be expected to threaten another individual's safety or physical or mental health.

As noted, several potential harms were cited in the breach reports to the OIPC. Three of those harms - identity theft, humiliation, and mental health stress (being encompassed by 'bodily harm') - are expressly listed in s. 36.3(2).

Despite these potential harms, the health authorities did not think that the requirement to notify affected individuals or report to the OIPC was met. Instead, they took the position that their notification to the OIPC was done so voluntarily. FHA also voluntarily notified two affected individuals and another individual who they identified as the personal representative of a deceased individual.

PHSA and VCH were also of the view that notification itself could cause harm to the affected individuals by re-traumatizing or re-victimizing them.

However, our risk assessment indicates that there is a further risk of harm associated with these breaches that goes beyond the gross invasion of privacy that has already occurred.

The language of "could reasonably be expected to" is used in several FIPPA provisions.[25] When considering the test imposed by this language, OIPC orders refer to the Supreme Court of Canada standard of proof for harms-based exceptions:

> This Court in *Merck Frosst* adopted the "reasonable expectation of probable harm" formulation and it should be used wherever the "could reasonably be expected to" language is used in access to information statutes. As the Court in *Merck Frosst* emphasized, the statute tries to mark out a middle ground between that which is probable and that which is merely possible. An institution must provide evidence "well beyond" or "considerably above" a mere possibility of harm in order to reach that middle ground: paras. 197 and 199. This inquiry of course is contextual and how much evidence and the quality of evidence needed to meet this standard will ultimately depend on the nature of the issue and "inherent probabilities or improbabilities or the seriousness of the allegations or consequences".[26]

For the reasons that follow, I am of the view that the expectation of significant harm in the present case is more than a mere possibility.

To find out about the medical history of patients, the employees who snooped contravened their legal and professional obligations, as well as the administrative and technical safeguards in place to protect that information. This raises some doubt about whether that information will be kept confidential in the future.

25 For example, see ss. 15, 16, 17, 18, 19, 21, 22 of FIPPA.

26 As cited at paragraph 8 in OIPC Order F17-57, 2017 BCIPC 62 (CanLII).

The fact that the breached information has already been disclosed by some of the snooping employees also indicates that the risk of subsequent violations is more than a theoretical possibility.

The likelihood of a worsening breach is further heightened by the ongoing community and public interest in the tragedy and those impacted by it.

I am also of the view that the snooping and possible consequences of the resulting breach are both very serious, which further supports a conclusion that there is a reasonable expectation of significant harm to the affected individuals. These harms are significant, as they involve highly sensitive personal information unlawfully accessed in the context of a traumatizing and tragic event.

The health authorities have said that the circumstances of the current breach are unprecedented. We understand this argument to mean that these breaches are not representative of what occurs more broadly in the healthcare system. However, in our view it is the unprecedented nature of what occurred that drove the underlying and ongoing curiosity that contributed to these breaches and heightens a reasonable expectation of significant harm.

I accept that VCH's and PHSA's position is based on a genuine concern for affected individuals and the desire to prevent any further stress on them. I also recognize that receiving the notice could be stressful - as it is in the case of any breach notification - however the evidence does not persuade me that notifying all of those impacted could reasonably be expected to result in "immediate and grave harm to the individuals' safety or physical or mental health", such that notice would not be required under s. 36.3(3)(a) of FIPPA.[27]

In contrast, notice of the breach would help to demonstrate to those affected by the breach that patient privacy is taken seriously and the health authorities are taking meaningful steps to address breaches. The health authorities can also use this opportunity to offer any further supports that may be available to the affected individuals. Moreover, notification would enable affected individuals to take steps that they feel are necessary to mitigate the kinds of significant harm contemplated by s. 36.3(2). Indeed, the affected individuals – not the health authorities - are the ones who are best placed to understand how the breach of their personal information may uniquely affect them. Notification also enables affected individuals to ask questions to the health authority about what happened and what options may be available in respect of their health records.[28]

27 *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165, s. 36.3(3)(a).

28 Notification includes information about what occurred, who can be contacted, the steps that the public body has or will take to reduce the risk of harm, and steps that affected individuals could also take to reduce the risk of harm. We have also listed contact information for the privacy offices of the health authorities in Appendix C.

Having considered the circumstances above, I find that there is a reasonable expectation of significant harm stemming from these breaches. Consequently, I am of the view that the health authorities had an obligation under s. 36.3(2) to complete notification.

In instances where notification is required by s. 36.3(2) of FIPPA, it must occur without unreasonable delay. VCH promptly reported to the OIPC but did not notify affected individuals as a result of their risk assessment. PHSA also did not notify affected individuals and reported the breaches to the OIPC approximately a month after they occurred. Conversely, while FHA did notify, that notice, and its report to the OIPC, were delayed at least one month after the breaches took place.

Recommendation 6

VCH and PHSA must provide notification as required by s. 36.3(2) of FIPPA, subject to the circumstances listed under s. 36.3(3).

Prevention

The final step in responding to a privacy breach is implementing measures to prevent a similar breach from occurring in the future.

I have found that the health authorities have reasonable security safeguards to protect against unauthorized access to personal information in the form of snooping. These safeguards are themselves preventative measures that should help to deter, detect, and respond to future snooping incidents.

However, in reviewing the breach reports and submissions for this investigation, I identified some measures that would strengthen those safeguards and the health authorities' processes for responding to breaches.

These measures include:

- more timely confirmation of breaches through improved audit capabilities and investigations;
- making greater use of technological safeguards and processes;
- revisiting training and privacy notices to strengthen communication about snooping; and
- ensuring that employee discipline is strong enough to meaningfully address snooping and deter others, including notifying professional regulatory bodies when needed or otherwise appropriate.

While breaches were promptly identified, the process of confirming those breaches was time consuming, which impeded the ability of the health authorities to contain breaches and to perform their obligations under s. 36.3 to notify the affected individuals and the OIPC without unreasonable delay.

The health authorities are taking steps to improve their audit capabilities. The current audit process involves the production and review of reports with thousands of lines of system activity and requires a significant amount of manual work. However, each of the health authorities and PHC has or will be implementing automated detection and auditing software that should help to address this issue.

To prevent snooping, real-time monitoring software must be populated with activity logs. The activities then must be compared to "rules" which indicate what is allowed behavior and/or what is abnormal behavior. These programs allow health authorities to much more efficiently monitor and review access to patient files.

In addition, if the system detects abnormal behavior, an alert can be immediately generated. Where possible, these systems should also be integrated with security systems, such as Security Information and Event Management systems, that can automate additional security controls, such as suspending access to records when suspicious activity is detected.

Once the automated monitoring system is in place and generating alerts, manual audits need to be conducted to determine if the alert was justified and whether the rules need to be refined. Manual audits are also periodically required to identify other potential situations where abnormal behaviour is occurring so further rules refinements can be made.

These improvements should help the health authorities detect and respond to snooping more generally (as opposed to the targeted auditing at issue here).

Recommendation 7

Continue existing efforts to deploy automated auditing software, with a focus on real-time alert generation and automated access prevention, where possible.

Recommendation 8

Review role-based access controls to prevent access rights from being inherited or mistakenly applied.

PHSA is also implementing a 'sensitivity alert' to use when a mass casualty incident occurs. This alert will be applied in circumstances where a patient requires a 'higher level of confidentiality' and can only be removed by their privacy department. When applied, an additional warning message will appear notifying of 'enhanced privacy monitoring.' These capabilities will also be made available to VCH and PHC, as shared users of the Cerner EMR.

FHA is similarly revisiting its process for appending extra privacy and confidentiality flags to make that process more readily available in its Meditech system and is working to implement more comprehensive notices in its Paris system. VCH is planning to revise its notice to make it more conspicuous to better address the possibility that employees have become accustomed to clicking on it.

VCH plans to implement additional administrative security measures. These include updating training and privacy notices to further emphasize snooping.

Other measures we heard include creating a procedure guideline for 'high profile' incidents, which will enable more efficient mobilization of resources to respond to a privacy breach, and increasing personnel resources to assist with responding to breaches.

While I support these additional measures, I also acknowledge that no system is perfect and that it may not be fully possible to prevent cases where an employee willfully violates their terms of employment, ethical and professional obligations, and the safeguards in place to restrict access to patient records.

Snooping on patient records is inconsistent with the terms of employment for healthcare workers and clear grounds for serious discipline. When it occurs, strong disciplinary measures are needed to address the behaviour and deter others who may be tempted to do the same.

Employees caught snooping were subject to a range of disciplinary measures, including:

- termination of employment;
- suspensions ranging from 1 to 10 days;
- notice to the employee's regulatory college;
- deprovisioning of access to electronic medical record systems; and
- letter of expectation/disciplinary letter issued.

In the context of a privacy breach, Commissioners have commented on whether discipline decisions of employers are sufficient. For example, Saskatchewan's Commissioner has recommended dismissal for instances of malicious snooping, as well as disclosure of the offending employee's identity to the individuals whose personal information was breached.[29] In Ontario, where there have been successful prosecutions for snooping, the provincial health law has recently been amended to allow for a fine of up to $200,000 for individuals and imprisonment for contravening the law.

The employees caught snooping in this case have or will be disciplined (except for two who resigned). And the discipline levied by PHSA and FHA appears consistent with their respective internal discipline guidelines.

In a digital records environment, the incentives to *not* snoop matter and strong disciplinary measures are a necessary tool for delivering privacy protections for patients. I am of the view that the discipline levied for snooping should lean towards stronger measures to better reflect the serious invasion of privacy and the breach of trust caused by snooping.

A breach of trust by a health professional is elevated because of the fiduciary nature of the professional's relationship with their patient.

29 *Regina Qu'Appelle Regional Health Authority (Re)*, 2014 CanLII 81862 (SK IPC), at paras 2, 3, 13, and 15 https://canlii.ca/t/gg5cv; *Saskatoon Regional Health Authority (Re)*, 2015 CanLII 46654 (SK IPC), at paras 18 and 27 https://canlii.ca/t/gkg4g.

Of those employees caught snooping, nearly half are subject to oversight by professional regulatory bodies in British Columbia.[30] These employees are also responsible for half of the snooping incidents discussed in this report.

The disciplinary actions applied to these employees ranged from a three-day suspension to termination. However, the health authorities did not report these disciplinary measures to employees' health profession colleges in all such cases.

Health profession colleges are responsible for setting and enforcing professional and ethical standards for their registrants, which include conduct that demonstrates honesty and integrity. Pursuant to s. 32.2 of the BC *Health Professions Act* (HPA), a registrant of a health profession college is required to report the conduct of another registrant, if on reasonable and probable grounds, the reporting registrant believes that the continued practice by the other person might constitute a danger to the public. This duty to report extends to persons (typically, employers) who take disciplinary action against a registrant if the discipline is based on a belief that the continued practice by the other person might constitute such a danger.

The HPA's reporting structure will be replaced when the relevant provisions of the *Health Professions and Occupations Act* (HPOA) come into force on April 1, 2026. The HPOA includes a different threshold for reporting to regulatory colleges. Specifically, the duty to report is triggered under the HPOA when the disciplinary action is based on a belief that the professional is not fit to practice or that their continued practice presents a significant risk of harm to the public. However, like the HPA, the HPOA does not expressly trigger a duty to report a breach of privacy, such as snooping. In contrast, health information legislation in Ontario requires the person or organization that has custody or control of personal health information to report privacy violations that result in a suspension or termination to the employee's professional college.[31]

If BC had language in its health professions legislation similar to Ontario's law, then the health authorities would have been required to report all such cases to professional colleges. This reporting can help shed light on the extent of these contraventions within the profession and inform professional standards and training. It would also be a meaningful security safeguard and consequence that deters this type of behaviour.

Employers, including health authorities, should seriously consider any harm or the danger to the public posed by an employee who continues to practice notwithstanding an intentional willingness to breach patient privacy.

30 College of Physicians and Surgeons; BC College of Nurses and Midwives and the College of Pharmacists of BC.

31 S. 17.1 of Ontario's *Personal Health Information Protection Act*, 2004, S.O. 2004, c. 3, Sched. A

The Province should similarly include a requirement for employers to report suspensions or terminations for privacy abuses to professional regulatory colleges in the HPOA, or more preferably, in stand-alone health information legislation.

Recommendation 9

Apply disciplinary measures for snooping that are strong enough to effectively sanction and deter snooping, including notifying regulatory colleges as required or appropriate.

Finding 3

Most aspects of the health authorities' breach response, including containment, risk assessment, and prevention meet the reasonable security safeguard requirement in s. 30. However, the lack of timely notification means that the overall breach response was not compliant with FIPPA.

Finding 4

FHA notified affected individuals and included elements in s. 11.1 of the FIPPA Regulation. However, that notice did not occur without unreasonable delay.

Finding 5

VCH and PHSA did not notify affected individuals or report to the OIPC without unreasonable delay as per the requirement in s. 36.3(2) and in the manner required by s. 11.1 of the FIPPA Regulation.

CONCLUSION

In total, 36 individuals were caught snooping on patient records 71 times. This abuses the trust of patients, their employers, and all those who rely on our health care system to keep their medical information private.

The health authorities have reasonable security measures to prevent snooping, however this report shows that those measures can be transgressed. When this occurs, the health authorities need to make reasonable containment efforts and assess the risk of harm to affected individuals.

The health authorities also needed to notify affected individuals if they are required to do so under s. 36.3(2) of FIPPA or if it would otherwise be appropriate. In the case of VCH and PHSA, this did not occur as both made the decision to not notify made based largely on the stress that such notification could cause. However, I am of the view that the fact that notification can cause stress does not alleviate VCH and PHSA from that responsibility. The argument that notification should not occur because it could be stressful can too easily obstruct the accountability of public bodies under FIPPA; patients' information belongs to patients, and they deserve to know when that information has been unlawfully accessed and misused.

All of the health authorities had elaborate safeguards and procedures to predict, detect, and respond to snooping. Obviously, as it still occurred, these were not perfect. I appreciate the open and collaborative approach that the health authorities took during this investigation, and that they have accepted and are implementing our recommendations, including taking additional preventative measures to strengthen existing processes and ensure disciplinary measures clearly sanction and deter snooping.

RECOMMENDATIONS

Recommendation 1: Clearly convey in privacy training that system activities are monitored and that discipline will be imposed for snooping.

Recommendation 2: Plainly state in confidentiality agreements that system use is monitored and consequences will be imposed for breaches of privacy and confidentiality.

Recommendation 3: The health authorities revisit their privacy notices. For Fraser Health this includes making greater use of Meditech privacy notices and working to implement a comprehensive confidentiality warning in its Paris system.

Recommendation 4: VCH and FHA update their privacy breach procedures to include information about mandatory breach notification requirements.

Recommendation 5: VCH develop disciplinary guidelines for privacy breaches that involve snooping.

Recommendation 6: VCH and PHSA must provide notification, as required by s. 36.3(2) of FIPPA, subject to the circumstances listed under s. 36.3(3).

Recommendation 7: Continue existing efforts to deploy automated auditing software, with a focus on real-time alert generation and automated access prevention, where possible.

Recommendation 8: Review role-based access controls to prevent access rights from being inherited or mistakenly applied

Recommendation 9: Apply disciplinary measures for snooping that are strong enough to effectively sanction and deter snooping, including notifying regulatory colleges as required or appropriate.

FINDINGS

Finding 1: Each of the cases reported by the health authorities and PHC represents a contravention of s. 25.1 of FIPPA.

Finding 2: VCH, PHSA ,and FHA employed reasonable security safeguards to protect against unauthorized access to personal information in the context of employee snooping.

Finding 3: Most aspects of the health authorities' breach response, including containment, risk assessment, and prevention meet the reasonable security safeguard requirements in s. 30. However, the lack of timely notification means that the overall breach response was not compliant with FIPPA.

Finding 4: FHA notified affected individuals and included elements in s. 11.1 of the FIPPA Regulation. However, that notice did not occur without unreasonable delay.

Finding 5: VCH and PHSA did not notify affected individuals or report to the OIPC without unreasonable delay as per the requirement in s. 36.3(2) and in the manner required by s. 11.1 of the FIPPA Regulation. This finding does not extend to any individual for whom notice is not required as per s. 36.3(3).

APPENDICES

Timeline of events
Provisions of FIPPA

APPENDIX A: TIMELINE OF EVENTS

April 26	• Assailant drives vehicle into crowd of people at the Lapu Lapu Day festival, killing eleven people and injuring dozens more. Some of the individuals who experienced the tragedy are sent to health care facilities across the Lower Mainland. • First VCH breach • First PHSA breach
April 27	• First FHA breach • VCH adds extra security controls to the records of patients who experienced the tragedy
April 28	• FHA starts adding names to watch list as they become known • VCH notifies PHSA of potential breaches in Cerner. PHSA also receives information about potential breaches by other organizations within the health authority. PHSA's privacy office begins audits of all affected systems and records through which access to affected patient personal information was possible.
April 29	• VCH Risk Management team issues memo to employees about privacy
April 30	• VCH reports breach to OIPC • PHC issues notice to Program Directors and Physician Program Directors in Saint Paul's Hospital Emergency and Internal Medicine about patient privacy and confidentiality in high profile incidents.
May 1	• FHA, VCH, PHSA, and PHC send a joint memo to all HIM employees about confidentiality
May 8	• FHA adds confidential flags to patient files in Meditech which results in a pop-up reminder that the chart is confidential
May 30	• FHA reports breaches to OIPC • PHSA reports breach to OIPC
June 20	• PHC reports breach to OIPC

APPENDIX B: PROVISIONS OF FIPPA

Unauthorized collection, use and disclosure of personal information prohibited

25.1 An employee, officer or director of a public body or an employee or associate of a service provider must not collect, use or disclose personal information except as authorized by this Act.

Protection of personal information

30 A public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized collection, use, disclosure or disposal.

Privacy breach notifications

36.3 (1) In this section, "privacy breach" means the theft or loss, or the collection, use or disclosure that is not authorized by this Part, of personal information in the custody or under the control of a public body.

(2) Subject to subsection (5), if a privacy breach involving personal information in the custody or under the control of a public body occurs, the head of the public body must, without unreasonable delay,

(a) notify an affected individual if the privacy breach could reasonably be expected to result in significant harm to the individual, including identity theft or significant

(i) bodily harm,

(ii) humiliation,

(iii) damage to reputation or relationships,

(iv) loss of employment, business or professional opportunities,

(v) financial loss,

(vi) negative impact on a credit record, or

(vii) damage to, or loss of, property, and

(b) notify the commissioner if the privacy breach could reasonably be expected to result in significant harm referred to in paragraph (a).

(3) The head of a public body is not required to notify an affected individual under subsection (2) if notification could reasonably be expected to

(a) result in immediate and grave harm to the individual's safety or physical or mental health, or

(b) threaten another individual's safety or physical or mental health.

(4) If notified under subsection (2) (b), the commissioner may notify an affected individual.

(5) A notification under subsection (2) (a) or (b) must be made in the prescribed manner.

Privacy breach notifications — affected individuals

11.1 (1) A notification under section 36.3 (2) (a) of the Act must

(a) subject to subsection (2) of this section, be given directly to each affected individual in writing, and

(b) include the following information:

(i) the name of the public body;

(ii) the date on which the privacy breach came to the attention of the public body;

(iii) a description of the privacy breach including, if known,

(A) the date on which or the period during which the privacy breach occurred, and

(B) a description of the nature of the personal information involved in the privacy breach;

(iv) confirmation that the commissioner has been or will be notified of the privacy breach;

(v) contact information for a person who can answer, on behalf of the public body, questions about the privacy breach;

(vi) a description of steps, if any, that the public body has taken or will take to reduce the risk of harm to the affected individual;

(vii) a description of steps, if any, that the affected individual could take to reduce the risk of harm that could result from the privacy breach.

(2) A notification may be given to an affected individual in an indirect manner if

(a) the public body does not have accurate contact information for the affected individual,

(b) the head of the public body reasonably believes that providing the notice directly to the affected individual would unreasonably interfere with the operations of the public body, or

(c) the head of the public body reasonably believes that the information in the notification will come to the attention of the affected individual more quickly if it is given in an indirect manner.

(3) If, under subsection (2), a notification may be given in an indirect manner, the notification must

(a) be given by public communication that can reasonably be expected to reach the affected individual, and

(b) contain the information set out in subsection (1) (b).

[en. B.C. Reg. 248/2022, Sch.]

APPENDIX C: HEALTH AUTHORITY CONTACTS

Fraser Health Information Privacy Office

100-13450 102 Ave
Surrey, BC V3T5X3
Phone: 236-484-1479
Email: informationprivacy@fraserhealth.ca

PHSA Privacy Office

200 - 1333 West Broadway, Vancouver, BC V6H 4C1
Phone:1-855-229-9800
Email: privacy@phsa.ca

Vancouver Coastal Health Information Privacy Office

11th floor, 601 West Broadway, Vancouver, B.C. V5Z 4C2
Phone: (604) 875-5568
Email: privacy@vch.ca

RESOURCES

Getting started

- Access to data for health research
- BC physician privacy toolkit
- Developing a privacy policy under PIPA
- Early notice and PIA procedures for public bodies
- Guide to OIPC processes (FIPPA and PIPA)
- Guide to PIPA for business and organizations
- Privacy impact assessments for the private sector
- Privacy management program self-assessment

Access (General)

- Common or integrated programs or activities
- Guidance for conducting adequate search investigations (FIPPA)
- Guidance on FIPPA's FOI process
- How do I request records?
- How do I request a review?
- Instructions for written inquiries
- PIPA and workplace drug and alcohol searches: a guide for organizations
- Proactive disclosure: guidance for public bodies
- Requesting records of a deceased individual
- Section 25: The duty to warn and disclose
- Time extension guidelines for public bodies
- Tip sheet: requesting records from a public body or private organization

Privacy (General)

- Direct-to-consumer genetic testing and privacy
- Disclosure of personal information of individuals in crisis
- Employee privacy rights
- Guide for organizations collecting personal information online
- Identity theft resources
- Information sharing agreements
- Instructions for written inquiries
- Obtaining meaningful consent
- Political campaign activity code of practice
- Political campaign activity guidance
- Privacy guidelines for strata corporations and strata agents
- Privacy-proofing your retail business
- Privacy tips for seniors: protect your personal information
- Private sector landlord and tenants
- Protecting personal information away from the office
- Protecting personal information: cannabis transactions
- Public sector surveillance guidelines
- Reasonable security measures for personal information disclosures outside Canada
- Responding to PIPA privacy complaints
- Securing personal information: A self-assessment for public bodies and organizations

Comprehensive privacy management

- Accountable privacy management in BC's public sector
- Getting accountability right with a privacy management program

Privacy breaches

- Privacy breaches: tools and resources for public bodies
- Privacy breach checklist for private organizations
- Privacy breach checklist for public bodies
- Privacy breaches: tools and resources for the private sector

Technology and social media

- Guidance for the use of body-worn cameras by law enforcement authorities
- Guidelines for online consent
- Guidelines for conducting social media background checks
- Mobile devices: tips for security & privacy
- PIPA and AI scribes: best practices for healthcare organizations in BC
- Tips for public bodies and organizations setting up remote workspaces
- Use of personal email accounts and messaging apps for public body business

Infographics

- FIPPA and the application fee
- How to identify deceptive design patterns
- How to make a complaint
- How to make an access request
- How to request a review
- Identifying and mitigating harms from privacy-related deceptive design patterns
- Responsible information sharing in situations involving intimate partner violence
- Requesting records of deceased individuals
- Tips for requesting records
- Transparency by default: information regulators call for a new standard in government review
- Tip sheet: 10 tips for public bodies managing requests for records

OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
FOR BRITISH COLUMBIA

PO Box 9038, Stn. Prov. Govt.
Victoria, BC V8W 9A4

Telephone: 250.387.5629
Toll Free in BC: 1.800.663.7867

Email: info@oipc.bc.ca