Information and Privacy Commissioner,
Ontario, Canada

Commissaire à l'information et à la protection de la vie privée,
Ontario, Canada

PHIPA DECISION 302

HR23-00193 and HR23-00279

Grand River Hospital[1]

September 12, 2025

Summary: Grand River Hospital (the hospital) reported two privacy breaches under the *Personal Health Information Protection Act, 2004* (the *Act*) to the Office of the Information and Privacy Commissioner of Ontario. Specifically, in two unrelated incidents, two hospital employees had each inappropriately accessed the personal health information (PHI) of a patient or patients by accessing Patient Lists they were not authorized to access.

To remediate the breaches, the hospital updated its *Breach Management: Privacy and Confidential Information Policy*, created a video to train its staff/agents on the topic of appropriate access and use of PHI via Patient Lists, and updated its annual privacy training with specific references to Patient Lists. Additionally, the hospital has enhanced and increased its communications to staff/agents regarding appropriate access to PHI via Patient Lists. Considering the remedial steps taken, a formal review of this matter will not be conducted under Part VI of the *Act*.

Statute Considered: *Personal Health Information Protection Act*, 2004, S.O. 2004, c. 3, sections 2, 3(1), 4(1), 10(1), 12(1) and 29.

Orders and Investigation Reports Considered: IPC Order HO-010

Cases Considered: PHIPA Decisions 163, 174, 204, and 264

[1] The name of the health information custodian changed after the breaches discussed in this decision were reported to the IPC. On April 1, 2025, Grand River Hospital and St. Mary's General Hospital merged into one entity and are now the Waterloo Regional Health Network.

BACKGROUND:

[1] In early 2023, under the *Act*, the hospital reported two separate privacy breaches to the Information and Privacy Commissioner of Ontario (the IPC). Each of the breaches involved an employee of the hospital looking at the PHI of a patient or patients by accessing Patient Lists in the hospital's Health Information System (HIS), called *Cerner*, without authorization.

[2] These matters moved to the Investigation Stage of the IPC's complaint process because they raised concerns about potential systemic issues at the hospital surrounding unauthorized access to PHI via the use of Patient Lists. Despite the hospital's remedial efforts in past breaches involving Patient Lists, theses incidents suggest that unauthorized accesses continued, calling into question the hospital's compliance with the *Act*.

The Reported Breaches

Reported Breach #1:

[3] On May 2, 2023, the hospital reported to the IPC that after a "Same Last Name" audit, a Clinical Extern had accessed a patient's PHI without authorization five times on March 13, 2023, and once on March 16, 2023. Specifically, the Clinical Extern had accessed this patient's PHI from a Patient List for an Intensive Care Unit while assigned to a different unit.

[4] The hospital detailed that the term "Patient List":

> is used at [the hospital] to describe a type of tool available in Cerner that assists its agents in locating the correct patients' charts. A patient list helps to organize and easily access patient data and can be built or viewed based on patient location, custom criteria or the provider relationship. Some patient lists, like those based on location, will be automatically populated by Cerner, while others need to be manually built by the user.

[5] Alongside patient names, the hospital stated that Patient Lists include personal health information such as results, orders, procedures, care plans, clinical diagnoses, laboratory results, recent vitals, assessments, education etc. Patient Lists are used by an agent[2] when their work requires accessing patient records for patients who are in that agent's "circle of care"[3].

---

[2] The *Act* defines "agent" as: "a person that, with the authorization of the [health information] custodian, acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian, and not the agent's own purposes, whether or not the agent has the authority to bind the custodian, whether or not the agent is employed by the custodian and whether or not the agent is being remunerated."

[3] Circle of Care: Sharing Personal Health Information for Health-Care Purposes | Information and Privacy Commissioner of Ontario

[6] The hospital explained that access to Patient Lists is obtained when a user of *Cerner* has access to the "User List" function/component in *Cerner*, from which the user can select any of the Patient Lists available and add them to their *CareCompass View*[4] as part of a "List Maintenance"[5] process. In its breach report, the hospital stated that the Patient Lists available are not restricted in any way by role or permission. The hospital explained that Patient Lists selected by a user through the "List Maintenance" process follow the user if they switch roles within the organization. The hospital stated that the user is responsible for removing Patient Lists they no longer require access to or are no longer authorized to access from their *CareCompass View*.

[7] The hospital's audit determined that the Clinical Extern had accessed documents in the patient's chart including but not limited to those under the following headings: Results, Order Profile, Orders, Procedures, Care Plan, Clinical Diagnoses, Recent Results, Results Review, Lab, Vitals, Assessments, Education and Notes.

[8] During a meeting following the hospital's investigation, the Clinical Extern stated that they understood they were not within the patient's *circle of care*, were not authorized to access their records, were contrite and sincerely apologized.

[9] The Clinical Extern acknowledged having made the inappropriate accesses noting that the patient was a friend/family of a friend and that they had accessed the records because the patient's family repeatedly asked questions about the patient's condition and because they were feeling emotional at the time. The hospital continued to monitor the Clinical Extern's accesses until the beginning of May 2023 and found no additional unauthorized accesses.

[10] The affected patient was notified of the privacy breach by letter on April 20, 2023.

[11] The hospital noted that the Clinical Extern had completed privacy training in May 2022, around the date of their initial hire. The hospital indicated that the Clinical Extern would have signed a *Confidentiality Agreement* during their onboarding.

[12] Following its internal guidelines for sanctions in privacy breaches, the hospital issued a written warning to the Clinical Extern and provided them with a *Learning Plan*. They were required to complete this plan within 30 days of receiving it, which the Clinical Extern did on May 8, 2023.

[13] After the breach, the Clinical Extern received privacy training on May 2, 2023, which included signing the hospital's *Privacy Pledge* and *Confidentiality Agreement*.

---

[4] *CareCompass* is software tool used by agents the hospital to view tasks and patient information, and complete documentation. The *CareCompass View* pane contains names and other patient details once a unit list is set up. The hospital's 33 Cerner Learning Guides detail this information.

[5] The "List Maintenance Process" refers to the actions taken by agents to create, update or remove a Patient List from their *Cerner* profile. Instructions are provided to agents through training tools prior to being granted access to *Cerner*.

Reported Breach #2:

[14] On June 14, 2023, the hospital reported to the IPC that after a "Same Last Name" audit, a Clinical Assistant was found to have accessed a patient's PHI without authorization, multiple times on one day in March 2023. The inappropriate access was a result of the Clinical Assistant accessing a Patient List for the Inpatient Surgical Unit while working in the Outpatient Oncology Clinic. The Clinical Assistant had accessed documents in the patient's chart including the following: Infectious Disease Risk Screening, Admission History Adult, Phone Call for Consults, Consult Note, ED Patient Education Note, Violence Assessment Tool, Pre-Anesthetic Questionnaire, and Intraprocedural and Postprocedural Records.

[15] Although at first the Clinical Assistant denied knowing the patient, the hospital's investigation determined that the Clinical Assistant was listed as an emergency contact for the patient. They were not in the patient's *circle of care* when they accessed the patient's records.

[16] During a meeting with the hospital, the Clinical Assistant confirmed they accessed the records and explained that they did so because the patient was their father, and his name was visible to the Clinical Assistant via the Patient List for the Inpatient Surgical Unit. The Clinical Assistant expressed remorse. The hospital conducted a general audit of the Clinical Assistant's access to all patients for the month of February 2023, and no other inappropriate access was identified. It continued to monitor the Clinical Assistant's accesses to their father's records until the end of March 2023 and found no additional unauthorized accesses.

[17] The affected patient was notified by letter on April 4, 2023.

[18] The Clinical Assistant first completed privacy training after they were hired, in October 2022. The hospital indicated that the Clinical Assistant would have signed a *Confidentiality Agreement* and the hospital's *Privacy Pledge* during their onboarding.

[19] Following its internal guidelines for sanctions in privacy breaches, the hospital issued the Clinical Assistant a written warning, suspended them from work and provided them with a *Learning Plan*. The Clinical Assistant was required to complete this plan within 30 days of receiving it, which they did, on May 30, 2023.

[20] After the breach, the Clinical Assistant received privacy training on May 9, 2023, which included re-signing a *Confidentiality Agreement* and the hospital's *Privacy Pledge*.

PRELIMINARY ISSUES:

[21] There is no dispute that the hospital is a "health information custodian" and that both the Clinical Extern and the Clinical Assistant were "agents" of the hospital as defined in the *Act*. There is similarly no dispute that the records accessed by the agents were

records of "personal health information" as defined by the *Act* within the custody or control of the hospital.

[22] Based on the information above, as a preliminary matter, I find that:

- the hospital is a "health information custodian" under paragraph 4.i of section 3(1) of the *Act*;
- the Clinical Extern and the Clinical Assistant were "agents" of the hospital, as that term is defined in section 2 of the *Act*;
- the records at issue contained "personal health information" under section 4(1) of the *Act*, which were in the custody or control of the hospital; and
- the hospital, via the accesses made by its agents (the Clinical Extern and the Clinical Assistant) used personal health information contrary to section 29 of the *Act*.

ISSUES:

[23] This decision addresses the following issues:

1. Did the hospital take reasonable steps to protect personal health information?
2. Is a review warranted under Part VI of the *Act?*

RESULTS OF THE INVESTIGATION:

Issue 1: Did the hospital take reasonable steps to protect personal health information?

[24] Health information custodians, when confronted with a breach of PHI, should take appropriate steps in response. These include containment of the PHI involved, notification to those affected, and investigation and remediation of the breach.

[25] Regarding the security of PHI, section 12(1) of the *Act* states:

> A health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal.

[26] In the matters at issue, the hospital identified the scope of both breaches and adequately notified the patients affected by the unauthorized accesses via letter. As such,

the remainder of my analysis focuses on the steps the hospital took to remediate the breaches, and in particular, the guidelines, practices and training it has put in place to protect patients' PHI as required under section 12(1) of the *Act*.

[27] In Order HO-010, the IPC stated that measures or safeguards must be reviewed from time to time to ensure that they continue to be "reasonable in the circumstances" to protect personal health information from theft, loss, and unauthorized use or disclosure and to protect records of PHI against unauthorized copying, modification, or disposal.

[28] The need to have proper safeguards in place has been set out in various IPC PHIPA Decisions discussing unauthorized access (also known as "snooping"), including more recently in Decisions 204, 202, 174 and 163. These decisions indicate that:

> Administrative and technical measures and safeguards are critical to protecting personal health information. The IPC has previously stated that, in order to comply with the requirements in section 12(1) of the Act and to take steps that are reasonable in the circumstances to protect personal health information, custodians must implement administrative and technical measures or safeguards, including privacy policies, procedures and practices, audit functionality, as well as privacy training and awareness programs and initiatives.

[29] In addition to the requirement to have proper safeguards in place, under section 10(1) of the *Act*, custodians that have custody or control of PHI must "have in place information practices that comply with the requirements of this Act and its regulations." To determine whether the hospital has taken reasonable steps to protect PHI, which includes having in place adequate information practices, the IPC's *Detecting and Deterring Unauthorized Access to Personal Health Information*[6] guidance document (the Guide) is informative.

[30] The Guide recommends that custodians implement the following measures to prevent or reduce the risk of unauthorized access:

- privacy policies and procedures;
- privacy training and awareness;
- privacy notices and privacy warning flags;
- confidentiality agreements;
- access management;

[6] https://www.ipc.on.ca/wp-content/uploads/Resources/Detect_Deter.pdf

- logging, auditing and monitoring;
- privacy breach management; and
- discipline.

[31] As part of my investigation, I reviewed the hospital's policies, procedures, training and other informational materials, focusing on information practices and procedures related to Patient Lists, as well as those centering on staff training, education and awareness with respect to the addition and removal of Patient Lists.

[32] I also reviewed previous similar incidents reported by the hospital. The IPC had concerns about the apparent systemic issue of continued unauthorized accesses via Patient Lists despite the hospital's remedial efforts in past breaches reported to the IPC.

Policies and Procedures

[33] Both agents who perpetrated the privacy breaches at issue in this investigation did so because they accessed Patient Lists for units to which they were not assigned, and for patients who were not in their *circle of care*.

[34] The hospital indicated that its privacy-related policies are a mechanism through which it ensures staff members know to only access Patient Lists related to their role. The hospital noted that its policies, *Privacy, Confidentiality and Information Security Policy* and *Release of Information Policy*, state that access to PHI is based on the principle of *need-to-know*.[7] The hospital explained that these policies are communicated to staff via mandatory annual privacy training and are always available on the hospital's intranet. The hospital stated that the concept of *circle of care* is covered in the hospital's annual privacy training.

[35] The IPC asked the hospital if it had a policy which clearly informs staff to only access the Patient Lists for the units that they are assigned to on a specific day. The hospital stated that "addressing patient lists is too detailed and specific to be included in a policy." The hospital highlighted that the purpose of a policy is to provide parameters and act as a guide for decision making on a particular topic. It noted that policies such as the ones referenced in the paragraph immediately above, provide the overall perimeters of expectations related to privacy and the use of its hospital systems/equipment, but they do not go into the granular details related to each system in use.

[36] The hospital initially advised the IPC that its policies would not be amended

[7] The hospital's *Privacy, Confidentiality and Information Security Policy*, at Appendix A, defines "Need to Know" as: "Access to PHI will be limited to only those employees/agents with a need to know such information for their job purposes (the "need to know" rule). Authorization is required before accessing, collecting, using, or disclosing PHI."

because of the two privacy breaches at issue. The hospital noted it was in the process of reviewing and updating its privacy policies to meet organizational needs. Its last policy update had occurred in 2019, when it launched *Cerner*. During this investigation, the hospital advised that it would be updating its standard "Health Information Network Provider language" as well as *Disciplinary Guidelines for Breaches of Privacy, Confidentiality and Security*.

[37] I reviewed some of the pertinent hospital policies and summarize the relevant portions below. The hospital's *Privacy, Confidentiality and Information Security Policy* states:

> As a Health Information Custodian (HIC) under the [*Act*], [the hospital] has an obligation to collect, use, retain and disclose personal health information (PHI) in a manner that protects the confidentiality and privacy of that information, while facilitating the effective provision of health care. […]
>
> [The hospital] relies upon the confidentiality, integrity, and availability of its information and technology systems to support business processes and the delivery of exceptional patient care. In compliance with legislation, regulatory directives and industry best practice, information and technology systems at [the hospital] will be appropriately safeguarded and utilized in a secure and controlled manner. [The hospital] will mandate and hold accountable [hospital] representatives to utilize information and assets legally, ethically and in a manner consistent with the values, vision and mission of the hospital.
>
> [The hospital] safeguards personal information (PI), personal health information (PHI), in accordance with the ten principles of the Canadian Standards Association's Model Code for the Protection of Personal Information, which is a national standard of Canada. The ten principles are interrelated, and [the hospital] will adhere to these principles as a whole.
>
> [The hospital] will make reasonable efforts within resource constraints to protect confidentiality, integrity and availability of data, information and systems by implementing processes, controls and defining accountability for regulatory compliance.

[38] This policy sets out the accountabilities and responsibilities of individuals in two sections, A and B:

A. the hospital's CEO and CPO; and

B. Staff, Management, Vice Presidents and Professional Staff.

In section B, the policy sets out that the individuals must be guided by the *Privacy & Information Security Principles* contained in Appendices A and B of this policy. The section

also states that these individuals must ensure that privacy and confidentiality agreements/attestations are signed annually.

[39] Appendix A of this policy is titled *Privacy Principles* and enumerates 10 such principles. Principle #5 discusses "Limiting Use, Disclosure, and Retention" and includes a definition of the principle of *need-to-know*.

[40] Appendix A also sets out the obligation of new employees to sign the hospital's *Privacy, Confidentiality and Security Agreement* (*Privacy Pledge)*. Further, it sets out that the hospital's *Confidentiality Agreement* will be signed by employees/agents annually upon completion of current privacy and information security awareness training, which reinforces duties and responsibilities under this policy.

[41] The hospital's *Release of Information Policy* sets out the principles that govern security, confidentiality, and access to PHI. This policy stipulates that "ensuring the confidentiality of patient information and the patient's right to privacy is the responsibility of everyone who has access to personal health information as appropriate to the role/responsibility that they fulfill in the organization." This policy also makes it clear that the use of PHI will be "on a **need-to-know** [emphasis in original] basis only as provided by PHIPA, including for health care purposes […]."

[42] In response to this investigation, the hospital committed to updating its *Breach Management: Privacy and Confidential Information Policy*. The hospital confirmed that this policy was updated and went live on April 2, 2025, highlighting that the list of examples of a "Level 2" privacy breach in Appendix A was updated. The update now includes the following information:

> **Level 2: Curiosity or Concern (no personal gain)**
>
> Often referred to as "snooping", this level of breach occurs when an agent intentionally accesses or discusses patient information for purposes other than the care of the patient or other authorized purposes but for reasons unrelated to personal gain. Examples include but are not limited to:
>
> • […]
>
> • An agent accesses information available via Patient Lists in the Health Information System (HIS) outside the principles of circle or care or need to know.

[43] In addition to the policies discussed above, the hospital also provided information regarding procedures. The hospital stated that procedures, such as its *Cerner Learning Guides*, are intended to provide the step-by-step instructions for specific tasks related to a particular health information system. It noted that *Cerner*-specific information is provided as part of the formal training agents receive before they can access *Cerner*. The hospital has 33 *Cerner Learning Guides* to train its staff to use *Cerner*. Each guide is for

a different role at the hospital (i.e. Ambulatory Nursing, Child and Youth Worker, Clinical Assist etc.)

[44] I reviewed some *Clinical Assist Cerner Learning Guides* to determine how access to Patient Lists is explained. These guides appear to instruct the learner on the technical steps to take within *Cerner* to add or remove a Patient List. They do not appear to advise staff to only access the patient lists that they are assigned to on a specific day, nor provide staff with guidance on the importance of privacy. They also do not appear to set out when it is appropriate to access and remove Patient Lists nor stipulate consequences for accessing Patient Lists without authorization.

[45] To address this, the hospital informed the IPC that its Digital Learning Team had devised an impactful approach to remind agents of the *circle of care* and *need-to-know* principles to reinforce that they should only be accessing the Patient Lists required for their current job duties/role: they created a video on the topic of Patient Lists, which I discuss below.

[46] The hospital noted that procedures related to accessing Patient Lists were updated in the form of the training for new agents, and information available to all agents on the hospital's intranet. I discuss the steps taken regarding training in the section immediately below.

Privacy Training, Education and Awareness

Training Video

[47] The hospital, via its Digital Learning Team, decided to create a short video specifically on the topic of Patient Lists. The video reminds the viewer of the principles of *circle of care* and *need-to-know* and provides best practices for using Patient Lists, including that active lists should reflect patients in one's *circle of care*, that if one is working across multiple units they should only access the Patient Lists of the units they are covering on that day, and that old Patient Lists are to be deleted when moving into a new role or when one is transferred to a different unit. The video includes a scenario and shows the steps needed to remove patient lists.

[48] The video was added to the *Cerner* Resources on the hospital's intranet on August 8, 2024, and to its *Cerner* Learning Modules and self-guided learning materials used to train students on September 13, 2024.

[49] The hospital indicated that, on August 8, 2024, it shared a link to the Patient Lists video (including where to find it on the hospital's intranet) with its Clinical Educators group (Education Practice Leads and Professional Practice Leads), "often the point people on various units for education, training and support."

Annual Privacy Training

[50] The hospital determined that the best mechanism to ensure that agents are trained on Patient Lists is to include the video in the hospital's annual privacy training. The hospital confirmed that as of February 11, 2025, any new agents undertaking annual training, or current agents renewing their annual training, are required to watch the Patient Lists video and read a scenario titled "*Is it a Breach?"* which includes an exercise for knowledge verification.

[51] The hospital provided me with information about their most recent annual training. This training covers a wide range of topics, with the following excerpts being of note in relation to the two privacy breaches at issue:

- Audits:
    - Performing audits is our process for assessing information handling practices, including using software to monitor access/use of PHI.
    - Random audits are performed and you are responsible for any activity that takes place using your credentials.
    - Privacy audits are routinely done to monitor who is accessing patient information and which screens are being viewed.
- Patient Lists:
    - You are not permitted any time to review your own health record or those of family/friends (outside of circle of care) using your hospital log-in. Accessing your own health record is considered a breach of hospital policy, while accessing the records of family/friends outside the circle of care is a breach of legislation.
    - Scenario 2: As a Stroke unit nurse temporarily in General Medicine, you check the Stroke Unit Patient List in Cerner, concerned about your Stroke patients' progress.
        - Is this a breach? Correct Answer: Yes, this is a breach. That is right! It is not appropriate to view and/or access PHI for patients that are on a different unit/department than the one you are actively assigned to. You are not part of the circle of care.
- Access to PHI:
    - Do I have to know this information to do my job? Access hospital information only when it directly relates to your job responsibilities and is

necessary to perform your job. Similarly, share hospital information with individuals only when it is necessary to do your job.

- When using or sharing patient or staff personal information, we are all expected to:
    - Be familiar with the Privacy Policies and their accompanying procedures
    - Ensure the 'need-to-know' principle is being met. Keep information sharing about a patient's health information or care within the 'circle of care'.

- Privacy Pledge: Agents are required to sign this *Privacy, Confidentiality and Security Agreement* at the end of their annual privacy training, prior to a final knowledge quiz. This agreement consists of 18 conditions which agents agree to abide by. Relevant conditions include the following:
    - **5**. I will not collect, use, or disclose any confidential information without authorization, nor will I discuss, divulge, or disclose confidential information about [the hospital] to others, unless it is necessary to fulfill my duties and responsibilities to [the hospital]. If I am unsure if I have the authorization of [the hospital] to access, use or disclose confidential information, I agree to seek clarification from my supervisor or the Privacy Office.
    - **6**. I will only collect, use or disclose (including: receive, look at, access, ask for, view, copy, record, print, read, listen, share with others) confidential information on a "need to know basis", and even then only the minimum amount required for my role or as I have been authorized to do so or as required by law.

Informal Communications

[52] According to the hospital, it controls access to Patient Lists via an "informal checklist" and email reminders. Senior staff members, such as the hospital's Manager, Professional Practice, Clinical Practice and Performance send out email communications to the hospital's Education Practice Leads and Professional Practice Leads (EPLs/PPLs) asking them "to remind or check in with transfers or new hires that have previously been students to ensure they have deleted patient lists from their previous positions or student placements."

[53] The hospital explained that it relies on its EPLs/PPLs to provide education, training and onboarding to Nurses and other allied health disciplines in their area of clinical specialty. It provides targeted privacy training to these leads with the expectation that information learned be then put into context for their teams.

Internal Publication "Grapevine Now"

[54] The hospital also indicated that it provides information regarding Patient Lists in its internal publication titled *Grapevine Now*. The hospital noted that it included a "privacy tip" titled "Avoid a privacy breach while using patient lists in Cerner!" in the April 29, 2024, issue of *Grapevine Now*. The privacy tip included the following information:

- only add the patient list of the unit that you are covering on your shift to your Cerner Profile
- if you are in the float pool, please make sure to only access the patient lists of the units you are covering on the given day, and remove those lists at the end of your shift or at the beginning of your next shift
- if you are monitoring the patient transfers for your unit, please make sure not to establish Patient-Provider Relationships with the patient lists of the other units
- if you take on a new role or are transferred to a different unit, please remove the patient list of your old unit from your Cerner profile

[55] The hospital noted that this privacy tip was provided as a best practice to ensure that agents understand the Patient List feature of *Cerner* and the hospital's expectations related to it. The hospital noted in an email to its EPLs/PPLs that it would appreciate it if they could mention this Privacy Tip in their next Huddle[8] and/or include it in an upcoming department/unit newsletter.

Formal Communications

[56] The hospital regularly sends other communications to its senior leadership team, Managers, Directors, Educators and Leaders reminding them of privacy issues. In an email from September 2024, the hospital reminded these individuals of the following:

> Privacy and confidentiality is key to the work we do, and it's important for team members not to use their employee access to review personal health information of friends or family admitted for care, which is against our policies. Instead, speak directly to the patient and consult their care team together, and please remember to also follow hospital visitor guidelines when visiting. This week's privacy poster is on the huddle board and highlights more details.

[57] To specifically address the issue of privacy breaches via the unauthorized access of Patient Lists, and in response to this investigation, the hospital integrated information regarding the management of Patient Lists in *Cerner* into its Town Hall meeting held on February 11, 2025. The hospital highlighted in this meeting that over the past few years

[8] The hospital indicated that huddles are short weekly meetings that include a team and its manager(s).

it had seen an increase in privacy breaches involving inappropriate access to Patient Lists in *Cerner* and stressed to staff the importance of incorporating the key privacy concepts of *circle of care* and *need-to-know* when accessing Patient Lists and any other systems containing sensitive information. In addition, the hospital played the video about Patient Lists at this Town Hall.

[58] The hospital also stated that the February 19, 2025, edition of *Grapevine Now* included a link to watch the recording of the Town Hall held on February 11, 2025.

[59] Further, the hospital sends out a bi-weekly email, called a *Huddle Helper*, to its staff. The hospital has explained that managers relay the messages from the *Huddle Helper* directly to their teams at short weekly meetings called huddles. In response to this investigation, an email was sent out on February 24, 2025, regarding Patient Lists which included a poster for managers to print and post on the "Huddle Board" of their unit with a QR code linking directly to the training video.

[60] Finally, the hospital indicated that it continues to provide education via presentations and that going forward, its intention is to make appropriate use of Patient Lists a subject of one of its "Privacy Tips" each year, featured in either its internal newsletter or in its *Huddle Helper*.

[61] My review of the hospital's information practices included not only whether the hospital has adequate privacy policies and training documents in place, but also how it communicated this guidance to employees. It is evident that since the time of these two breaches, the hospital has been communicating with increased visibility to its agents/staff the importance of solely accessing Patient Lists when authorized.

Confidentiality Agreements:

[62] An important administrative safeguard in protecting patients' PHI is requiring agents to sign a confidentiality agreement on a regular basis to acknowledge privacy obligations and expectations, including the consequences of a privacy breach.[9]

[63] The hospital provided the IPC with copies of the *Confidentiality Agreement* signed by the Clinical Extern and Clinical Assistant. This agreement states that the staff member "shall ensure that confidential information is not inappropriately accessed, used, or disclosed" and that violations include, but are not limited to "accessing confidential information that I do not require for the purposes of fulfilling my duties and responsibilities to Grand River Hospital." Consequences for violations are set out and include corrective action, termination of employment, loss of privileges, contract termination, or other appropriate action.

---

[9] See Information and Privacy Commissioner of Ontario (January 2015), *Detecting and Deterring Unauthorized Access to Personal Health Information*, retrieved from < https://www.ipc.on.ca/en/resources-and-decisions/detecting-and-deterring-unauthorized-access-personal-health-information >.

[64] The hospital explained that all employees, professional staff and volunteers must sign a *Confidentiality Agreement* as part of their onboarding and must also sign a *Privacy Pledge* at hire and annually thereafter with privacy training. The agreement is embedded in the annual training virtual module and requires acknowledgement for completion.

Privacy Warning Flags:

[65] Privacy notices and warning flags in electronic record systems serve to remind health information custodians and their agents about their obligations to protect PHI and the potential consequences of accessing PHI in contravention of the *Act*. They are useful tools in deterring privacy breaches as they may prevent or reduce the risk of unauthorized access.[10]

[66] The hospital makes use of such a flag. It indicated that *Cerner* contains a privacy warning that agents must view before accessing PHI. The warning states the following:

> Caution:
>
> In accordance with the Personal Health Information Protection Act (PHIPA) and GRH/SMGH privacy policies, it is not appropriate to access patient health information (PHI) unless you are currently withing the circle of care providing care to the specific patient, or assisting in the provision of care to that patient. Inappropriate collection, access, use or disclosure of PHI will be considered a breach of confidentiality and will result in disciplinary action, being reported to your regulated health professional college and/or being reported to the Information and Privacy Commissioner of Ontario. By continuing into this system, you accept the terms of use.

Audit Functionality:

[67] The hospital stated that it conducts monthly scheduled as well as random audits to monitor compliance with its policies and identify inappropriate access to PHI. It also carries out requested audits (as required by patient request or incident investigation) on patients and staff in *Cerner*. The hospital has an *Audits of Health Information Systems Policy*.

[68] The hospital noted that at this time it does not have the ability to complete an audit of staff who access Patient Lists for units that they are not assigned to, stating that audits currently available are not intended to be used in this way. The hospital stated that it "speculates" that staff scheduling systems would somehow need to interface with the hospital's HIS to build an audit that could be run to detect agents accessing information from units they are not assigned to for a specific shift. The hospital stated: "If these systems can communicate, this would still be a complicated technical feat to achieve as we do not believe that the staff scheduling systems necessarily list the specific

[10] PHIPA Decision 110 at paragraph 100.

units of the hospital in the same way that Cerner does."

CONCLUSION:

[69] According to the information before me, these two breaches came to the hospital's attention because of continued inappropriate accesses through Patient Lists, despite the hospital's remedial efforts in similar past breaches. In my view, the hospital has a responsibility to demonstrate that it has taken steps to prevent similar situations from arising in future and that it has met its obligation to take reasonable steps to protect personal health information.

[70] Based on my review of the hospital's policies, particularly the addition of information regarding Patient Lists to its *Breach Management: Privacy and Confidential Information Policy* and appendices, as well as the hospital's updated privacy training and targeted informational materials, I am satisfied that the hospital has implemented the administrative, technical and physical safeguards necessary to comply with the requirements in sections 10(1) and 12(1) of the *Act*. The hospital has taken adequate measures to communicate the need to protect patients' privacy, and direct employees not to access personal health information unless necessary in the course of their jobs.

Issue 2: Is a review warranted under Part VI of the *Act*?

[71] For the reasons noted above, I am satisfied that the hospital has taken appropriate steps to address the privacy concerns raised by the two breaches without the need to proceed to the adjudication stage of the IPC's process at this time.

DECISION:

Section 58(1) of the *Act* sets out the Commissioner's discretionary authority to conduct a review as follows:

> The Commissioner may, on his or her own initiative, conduct a review of any matter if the Commissioner has reasonable grounds to believe that a person has contravened or is about to contravene a provision of this Act or its regulations and that the subject-matter of the review relates to the contravention.

In accordance with my delegated authority to determine whether a review should be conducted under section 58(1) of the *Act,* and for the reasons set out above, I find that a review is not warranted. No review will be conducted under Part VI of the *Act*.

Original Signed by: September 12, 2025

Alexandra Madolciu
Investigator