Information and Privacy Commissioner,
Ontario, Canada

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

PHIPA DECISION 264

Complaint HR22-00017

A Public Hospital

November 6, 2024

Summary: A public hospital reported a privacy breach under *PHIPA* to the Office of the Information and Privacy Commissioner of Ontario (IPC). The breach involved a radiologist with privileges at the hospital who accessed patients' health records without authorization. The affected patients included the radiologist's sister-in-law, who brought the privacy breach to the attention of the hospital, as well as members of her family.

As an agent of the hospital, the radiologist's actions were an inappropriate use of personal health information by the hospital contrary to section 29 of *PHIPA* which sets out limits on and requirements for the use of this information.

In response, the hospital took steps to investigate, contain and remediate the breach. The hospital also provided the appropriate notification in the circumstances, disciplined the radiologist and reported him to the College of Physicians and Surgeons of Ontario.

Despite this, the IPC had concerns about the hospital's ability to detect and deter unauthorized access to patients' health records in relation to its EHR systems. These systems were not built from a privacy audit perspective and the hospital only became aware of the breach because of a privacy complaint made by the radiologist's sister-in-law to another regional hospital about him.

At the time of the breach, the hospital's EHR systems had inherent limitations and, generally, did not display a privacy notice or warning flag. For these reasons, the investigator finds that the hospital did not take steps that are reasonable in the circumstances for the security of personal health information against unauthorized use as required by section 12 of *PHIPA*. However**,** given the hospital's response to the breach and implementation of privacy warning flags in its EHR

systems, the investigator finds that a formal review of this matter under Part VI of *PHIPA* is not warranted.

Statutes Considered: *Personal Health Information Protection Act, 2004, S.O. 2004, c. 3; Sched. A.*, sections 2, 3(1), 4(1), 12, 29 and 58(1).

BACKGROUND:

[1] A public hospital (the hospital) reported a privacy breach under the *Personal Health Information Protection Act, 2004* (*PHIPA*) to the Information and Privacy Commissioner of Ontario (the IPC or this office).

[2] The breach involved a radiologist with privileges[1] at the hospital who had snooped into patient health records. Some of the affected patients were known to the radiologist who explained that he had viewed the records out of curiosity.

[3] In July 2021, the hospital became aware of the breach after the radiologist's sister-in-law complained to another local hospital, at which she was a patient and where the radiologist also had privileges (the local hospital), that he had inappropriately accessed her health records.

[4] An investigation by the hospital, the local hospital and the privacy team for the region (the Regional Privacy Team) into the sister-in-law's complaint found that, between 2015 and 2021, the radiologist had inappropriately accessed health records relating to her, her husband, their daughter and 17 other patients (together, the affected individuals) numerous times. The investigation also determined that he did so by searching for their names in the regionally shared electronic health record (EHR) systems using a radiologist home workstation or, since 2019, the hospital's devices.

[5] The affected individuals' information accessed by the radiologist included their name, address, phone number, date of birth, health card number, family physician, visit history, unit, registration date, discharge date, encounter type, attending physician, facility, reason for visit, exam imaging and medical reports (together, the affected individuals' information).

[6] In response to the breach, the hospital notified its appropriate staff and worked with both the local hospital's privacy team and the Regional Privacy Team to determine the scope. This involved having discussions with some of the affected individuals and the radiologist, as well as auditing his accesses in the EHR systems.

---

[1] "Hospital privileges" is a term generally used to indicate the appointment of a physician to the staff of a hospital. Hospital privileges provide a physician with access to the hospital's facilities, and they also specify the types of procedures a physician may perform in the hospital. The process for granting, changing and terminating hospital privileges are set out in a hospital's by-laws. See the College of Physicians and Surgeons of Ontario's Glossary of Terms.

[7] The systems audited included Cerner/Power Chart (Cerner), as well as AGFA picture archiving and communication system (PACS) and General Electric (GE) PACS (together, the PACSs). The audits determined that the radiologist had accessed the affected individuals' information without authorization using Cerner and GE PACS.

[8] To contain the breach, the hospital implemented a Denial of Access[2] in August 2021 to prevent the radiologist from accessing the sister-in-law's health record in Cerner. The hospital also informed him of the audit results and its ongoing investigation at that time and audited his accesses to patient health records daily. In September 2021, the hospital also developed an interim process in which the radiologist self-reported the tasks that he performed each shift within Cerner to his Department Chief.

[9] As a result of the breach, the hospital took certain disciplinary actions against the radiologist and notified the College of Physicians and Surgeons of Ontario (the CPSO).[3]

[10] According to the hospital, all the affected individuals were successfully notified of the breach. Notification letters were sent to them by email and registered mail, and included the radiologist's name, a description of the breach's nature and scope, a description of the affected individuals' information, the steps taken to address the breach, contact information for the hospital's breach contact, and a statement informing them of their entitlement to make a privacy complaint about the matter to the IPC. Because of the breach, this office received complaints from some of the affected individuals.

[11] Further, the hospital sent notification letters to the local hospital and the other hospitals within the region that share health records in Cerner and the PACSs.

[12] In addition to a notification letter, the hospital also sent the affected individuals an apology letter written by the radiologist. In this letter, the radiologist acknowledged that he had accessed their information without authorization and apologized for doing so. The radiologist also confirmed that he did not disclose their information to any third parties and that he would not perform an unauthorized search again.

[13] With respect to remediation, the hospital reviewed its privacy policies and procedures, as well as its physician credentialing process to identify areas where privacy and *PHIPA* education could be enhanced.

[14] Despite the above steps taken by the hospital, this office had concerns about its ability to detect and deter unauthorized access to personal health information (PHI) relating to Cerner and the PACSs. As such, this matter moved to the Investigation Stage

[2] The hospital explained that, when placed on a specific user, a Denial of Access prevents the user from opening a specific patient's chart in Cerner.
[3] Section 17.1of *PHIPA* that discusses notice to a "College" such as the CPSO.

of this office's complaint process.[4]

PRELIMINARY ISSUES:

[15] The hospital does not dispute that, under *PHIPA*, it is a "health information custodian" and that the radiologist is its "agent".[5]

[16] The hospital also does not dispute that, under *PHIPA*, the affected individuals' information is "personal health information" in its custody or control, and that the radiologist's viewing of this information was an unauthorized "use" of PHI.

[17] Accordingly, as a preliminary matter, I find that:

- the hospital is a "health information custodian" under paragraph 4.i. of section 3(1) of *PHIPA*,
- the radiologist is an "agent" of the hospital under section 2 of *PHIPA*;
- the affected individuals' information is "personal health information" under section 4(1) of *PHIPA*; and
- because the radiologist viewed the affected individuals' information without authorization under *PHIPA*, the hospital used this PHI contrary to section 29 of *PHIPA*.

ISSUES:

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

DISCUSSION:

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

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

> A health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's

[4] Part III-Custodian-Reported Files and IPC-Initiated Files of the IPC's Code of Procedure for Matters under the *Personal Health Information Protection Act, 2004*.
[5] See sections 2 and 3 in *PHIPA* for the definitions of these terms.

> 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.

[19] This office has stated that, under this section, custodians have a duty to respond adequately to a privacy breach complaint, and that a related obligation is the duty for custodians to implement and comply with information practices, including administrative, technical and physical safeguards or measures with respect to PHI in their custody or control.[6] Custodians must also maintain and review their practices to protect an individual's privacy from time to time to ensure that they continue to be "reasonable in the circumstances", as well as identify risks to privacy and take reasonable measures to reduce or eliminate such risks and mitigate the potential harms that may arise.[7]

[20] In this matter, the radiologist was able to access the affected individuals' information without authorization by searching for their names in Cerner and GE PACS. Accordingly, it must be determined whether the hospital had reasonable measures in place at the time of the breach to ensure that their information was protected against this unauthorized use.

[21] As part of my investigation, I reviewed the hospital's policies, procedures, training materials and other informational materials.

Auditing and Monitoring

[22] With respect to Cerner and the PACSs, auditing and monitoring of all accesses to electronic PHI records in these EHR systems is important to ensure the privacy of individuals and the confidentiality of their PHI.[8]

[23] As a technical safeguard, this office has stated the following about the importance of audit functionality in the health sector:

> As in other industries, audits play an important role in the health sector. Auditing of electronic information systems is particularly important in ensuring that the privacy of individuals and the confidentiality of personal health information are protected. Audits are essential technical safeguards for electronic information systems. They can be used to deter and detect collections, uses and disclosures of personal health information and the copying, modification or disposal of records of personal health information that contravene [*PHIPA*]. As such, they help to maintain the integrity and confidentiality of personal health information stored in electronic

---

[6] PHIPA Decision 110.
[7] PHIPA Decisions 64, 70, 163 and 174; and IPC Orders HO-010 and HO-013.
[8] The IPC's *Detecting and Deterring Unauthorized Access to Personal Health Information* guidance document. Available online: https://www.ipc.on.ca/en/media-centre/blog/detecting-and-deterring-unauthorized-access-personal-health-information.

> information systems. The ability to conduct audits of personal health information and the activities of agents or users (referred to in this section as users) in an electronic information system also ensures that a health information custodian is able to respond to requests from patients for information about who has collected, used or disclosed their personal health information.
>
> In order to be effective, audits require analyzable data about the full extent to which users collected, used, disclosed, copied, modified or disposed of personal health information within a given time period. If such data is not available or is only available in part, then a health information custodian will not be able to conduct a complete audit in relation to the personal health information stored in its electronic information system.[9]

[24] Of particular concern to this office in this matter, the hospital reported that Cerner and AGFA PACS, as well as GE PACS, were not constructed from a privacy audit perspective and that auditing them is both challenging and time consuming. The hospital explained that these difficulties are increased when auditing GE PACS because it is a legacy platform that is no longer supported.

[25] To detect and deter unauthorized access to PHI, the hospital conducts both random and targeted audits in Cerner and AGFA PACS. However, due to the hospital's limited auditing capabilities, these audits are conducted in collaboration with and primarily by:

- the Regional Privacy Team in Cerner;
- the Regional Privacy Team until February 2023 and, presently, by the Ontario Clinical Imaging Network (OCINet)[10], in AGFA PACS; and
- the Regional Privacy Team until February 2023 and, presently, by the OCINet, in GE PACS.

[26] According to the hospital, this external reliance on the Regional Privacy Team and OCINet is not unique because the other regional hospitals that share health records in Cerner and the PACSs have the same reliance.

---

[9] IPC Order HO-013 at page 23.

[10] OCINet was formed in April 2022 with the consolidation of three diagnostic imaging repository programs (i.e. HDIRS, NEODIN, SWODIN), and created to execute Ontario's medical imaging digital health strategy. OCINet enables the secure storage and retrieval of image records, supports hospitals and integrated community health services centres (ICHSCs) (also known as independent health facilities, or IHFs), and connects radiologists, referring physicians, and specialists with their patients' images province-wide. For more information, visit: https://ocinet.ca/about-us/about-ocinet/.

Cerner

[27] The radiologist was able to access some of the affected individuals' information (i.e. the visit history information) without authorization by searching for their names in Cerner.

[28] When searching for a patient by (full) name in Cerner, the hospital explained that the user can view the patient's visit history information because it is displayed on the resulting (visit history) screen. As such, there is no need for the user to "double-click" into a patient's health record to access this PHI.

[29] Further, when a Cerner user conducts a partial name search, the hospital advised that they could view more patient records than the one being searched for. According to the hospital, this possible outcome is due to Cerner's design.

[30] The hospital acknowledged that this outcome may result in the disclosure of more PHI than necessary. To limit such disclosure, when searching for a patient by name, the hospital advises users to use a minimum of two identifiers. Further, the hospital explained that such outcome serves as a patient accuracy function where the user may need to see more information to identify the patient being searched for.

[31] When auditing users' name searches in Cerner, the hospital advised that a broad name search would, generally, flag the Regional Privacy Team's attention and, as a result, the audit timestamps would be reviewed to determine whether a significant amount of time had passed before the user made the next "click" and moved on to the next step in their work.

[32] Where the user clicks almost immediately, the Regional Privacy Team would assume that the user did not spend time perusing the PHI. However, where the user does not move on for multiple seconds/minutes, the Regional Privacy Team would assume that the user was interrupted or doing something more suspicious. Such delay would trigger an investigation into the user's access of PHI.

[33] To limit a user's access in Cerner, the hospital advised that this can only be done by manually applying a consent directive (i.e. a "lockbox") [11]on a per visit basis to a patient's health records and by Denial of Access.

[34] To detect and deter unauthorized access, Cerner has 219 different types of audits available but before using them, the hospital advised that there are many considerations, which include that all audits must be manually initiated and the data manually sorted, and many of the audits contain so much data that it is impossible to run them to audit a lengthy period. Moreover, the hospital explained that, although auditing supplies the data, a privacy resource is required to review the data, investigate the audit events, and

[11] For more information about a "lock-box" visit online: https://www.ipc.on.ca/en/resources-and-decisions/fact-sheet-08-lock-box-fact-sheet.

determine whether a breach occurred.

[35] As such, the hospital advised that if a patient does not raise a specific privacy concern, the "red flags" that would identify a potential inappropriate access could easily be missed.

[36] The hospital also advised that many of the Cerner audits do not show the users who have not taken the step of opening a patient health record in this EHR system. This is the reason why the Regional Privacy Team did not initially identify the radiologist's inappropriate accesses. He only viewed the affected individuals' visit history information but did not open their patient health records.

[37] Essentially, with respect to the hospital's auditing and monitoring of all accesses to PHI in Cerner, the hospital advised that the Regional Privacy Team is limited on a proactive basis to prevent unauthorized access to PHI by users such as the radiologist. The hospital explained that this deficiency results from Cerner's lack of an intelligent means to limit, flag, or shut off access for a possible unauthorized access to PHI. Accordingly, the hospital acknowledged that it is limited to reactive and highly manual audits, such as the ones that were performed to investigate the sister-in-law's concerns about the radiologist.

[38] Further, the hospital advised that this deficiency cannot be addressed by Cerner's vendor at this time and that, regionally, there are approximately 5,000,000 transactions per day logged in Cerner's auditing tool, with 60,000 to 70,000 of those being searches. According to the hospital, approximately 99% of the searches are appropriate.

[39] The hospital explained that, presently, Cerner's auditing tool is basically recording all transactions and searches but is not intelligent enough to link a patient to staff outside of user specific audits. Moreover, because all audits must be manually interpreted, the hospital must determine whether the recorded searches are appropriate by matching staff to patients.

[40] In the hospital's view, to do this for 60,000 – 70,000 searches daily would be beyond the capacity of any privacy office, including the Regional Privacy Team. As such, the hospital believes that, presently, it is only practical to undertake interpreting the data supplied by an audit in Cerner where a patient raises a specific privacy concern.

AGFA PACS and GE PACS

[41] Since July 2018, the hospital has used AGFA PACS. Before then, it used GE PACS which was decommissioned in 2018.

[42] Presently, OCINet manages AGFA PACS. Before April 2022, the hospital advised that the PACSs were managed by the Southwestern Ontario Diagnostic Imaging Network (SWODIN) and that SWODIN was managed by the local hospital and the Regional Privacy Team.

[43] The radiologist was able to access some of the affected individuals' information without authorization by searching for their names in GE PACS and then opening their patient records.

[44] The hospital advised that a name search by a user in the PACSs will return a viewable list of patient PHI, but not the patient's final interpreted report or associated exam images. The hospital also advised that this type of search is not captured by audit tools in the PACSs. However, where a patient's report or exam images are accessed, the hospital advised that such access can be audited, and the results will show the user's identification.

[45] Accordingly, in this matter, the audit results from GE PACS included detailed information about the specific name searches that the radiologist conducted because he accessed the affected individuals' exam imaging and/or medical reports.

[46] This office asked the hospital about the possibility of developing and implementing an auditing tool for name searches conducted in the AGFA PACS. In response, the hospital advised that the auditing functions and tools for the AGFA PACS are by system design and that, through OCINet, a formal enhancement request has been made to the vendor to further develop an auditing function in this PACS to capture name searches.

Radiologist Home Workstation

[47] The hospital advised that its radiologists are also required to work remotely. To do so, they use a radiologist home workstation that they can purchase, or the hospital can provide to them.

[48] The workstation includes a computer and monitors that are dedicated to and designed specifically for working remotely and, with respect to privacy and security measures, includes an encrypted hard drive, remote access to Cerner and AGFA PACS through a virtual private network, as well as username and password protection.

[49] Regarding the radiologist's inappropriate accesses of PHI, he was appointed to the hospital's professional staff in January 2013 with privileges but did not practice on-site until May 2019. As such, the hospital explained that, before May 2019, the radiologist would have accessed the affected individuals' information in Cerner and GE PACS using a radiologist workstation and not devices at the hospital.

Privacy Notices and Privacy Warning Flags

[50] Privacy notices and warning flags remind custodians and their agents of their obligations to protect PHI and of the consequences of accessing this information in contravention of *PHIPA*. As such, they may prevent or reduce the risk of unauthorized

access to PHI.[12]

[51] At the time of the breach, the hospital reported that Cerner did not have a privacy warning flag. As a remedial step, the hospital raised this issue with the Regional Privacy Team and efforts were made to implement a privacy warning flag in this EHR system.

[52] Implementation was completed in December 2023 and the warning, which cannot be bypassed, reminds users that "your access of patient data in the EHR is monitored. Unauthorized use, collection or disclosure of patient data is a serious breach that may result in disciplinary action and/or other serious consequences."

[53] The hospital also reported that, at the time of the breach, radiologists did not see the privacy warning flag in AGFA PACS because they accessed the Enterprise Imaging section of this system. The hospital explained that AGFA PACS users entering the "Xero" section of AGFA PACS (which is broadly available) would see this warning requiring their confirmation that they understand corporate privacy policies and will comply with Ontario privacy legislation and only use PHI to provide or assist in the provision of care. This warning also reminds users that misuse of PHI "may be cause for disciplinary action up to and including termination of employment/contract or loss of appointment or affiliation".

[54] As a remedial step, a request was made to the vendor in May 2022 to see whether a privacy warning flag could be implemented in the Enterprise Imaging section of AGFA PACS used by radiologists. The hospital confirmed that a privacy warning has been implemented in this section informing them and any other user that accessing PHI is confirmation that "you will only collect use or disclose PHI for the provision of healthcare and/or support of the provision of healthcare in accordance with your organization's privacy policies."

[55] With respect to the retired GE PACS, the hospital reported that it is not aware if there was a privacy warning flag in this EHR system at the time of the breach because information regarding this was not retained.

Privacy Policies and Procedures

[56] Custodians should have privacy policies and procedures in place to detect, prevent and reduce the risk of unauthorized accesses to PHI by their agents.[13]

[57] The hospital provided this office with copies of its Confidentiality Policy, Privacy Policy, and Acceptable Use of Information Technology (IT) Resources Policy (together, the hospital's privacy policies) in place, presently, and at the time of the breach.

[12] See footnote 7.
[13] See footnote 7.

The Confidentiality Policy

[58] The Confidentiality Policy's sets out the "the hospital's expectations and standards of behaviour related to confidentiality" and aims to "safeguard and protect the privacy of patients, staff and hospital affiliates, according to legislative requirements."

[59] This policy considers patients' and their families' PHI to be confidential and makes the hospital's staff responsible for using this information only as authorized. The policy also sets out disciplinary action that the hospital may take against staff for misuse of PHI.

[60] Further, the Confidentiality Policy requires that the hospital's staff review it "and sign a Confidentiality Agreement before they receive hospital privileges or begin their work at the hospital", as well as participate in the hospital's privacy and confidentiality education program.

[61] With respect to confidentiality agreements, requiring agents sign them on a regular basis may help to prevent or reduce the risk of unauthorized access to PHI. [14]

[62] The hospital's confidentiality agreement is agreed to and signed by staff on an annual basis and requires their confirmation that they have read and understood the Confidentiality Policy and commit to holding patient PHI in confidence during and after their employment or affiliation with the hospital. This agreement also requires that the hospital's staff confirm that they understand that misuse of confidential information may result in disciplinary action being taken against them.

The Privacy Policy

[63] The Privacy Policy applies to all the hospital's staff and requires that they access and use confidential information only as authorized.

[64] More specifically, this policy requires that the hospital:

- ensure that its staff, agents and affiliates are aware of their duties related to privacy;
- protect the safety and respect the confidentiality of PHI through appropriate access safeguards; and
- implement safeguards to protect PHI against unauthorized access.

Acceptable Use of IT Resources Policy

[65] The Acceptable Use of IT Resources Policy details "the acceptable use of the hospital's IT resources, which include all computer and communications equipment

[14] See footnote 7.

installed on the hospital's property or otherwise provided by the hospital."

[66] Auditing and monitoring of access to PHI can be an effective deterrent to unauthorized access if all agents are made aware that all their activities in relation to electronic PHI records will be audited and monitored on an ongoing targeted and random basis.[15]

[67] This policy makes it clear that "users of the hospital's IT resources are responsible for compliance with applicable organization policies and procedures, e.g. privacy and confidentiality, ..." and that the hospital, without prior notice, has the right to audit and monitor these systems.

[68] Further, the Acceptable Use of IT Resources Policy requires that users comply with it when using their own devices (such as a radiologist home workstation) to access the hospital's IT resources. This policy also sets out unacceptable uses of the hospital's IT resources which include accessing patient PHI records "where access is not required to perform the duties for an which an individual is employed by or affiliated with the organization, including the user's own records and those of family and friends."

Professional Staff

[69] The hospital advised that, when applying for privileges, professional staff (which includes the radiologist) must review the Confidentiality Policy and confirm that they have done so by signing a confidentiality agreement.

[70] Moreover, professional staff must review the hospital's privacy policies annually and confirm that they have done so as part of its reappointment process when applying to be a professional staff member. Further, since 2019, the hospital advised that these applications have become more specific by requiring all professional staff to confirm that they have read, understood, and agreed to comply with the hospital's privacy policies, as well as undertaken the related training when submitting their annual application. [16]

[71] With respect to the radiologist, as part of his initial appointment to the hospital's professional staff in 2013, he was required to review the Confidentiality Policy and sign a confidentiality agreement. Further, the hospital advised that he acknowledged and agreed to abide by the confidentiality agreement and the hospital's privacy policies on an annual basis during the period in which he accessed the affected individuals' information without authorization.

Privacy Training

[72] Comprehensive privacy training is an essential tool to reduce the risk of

[15] See footnote 7.
[16] The hospital advised that, for the 2020/2021 credentialing year, reappointment was automatic and its professional staff did not have to complete this application due to COVID-19.

unauthorized access to PHI.[17]

[73] The hospital conducts privacy training annually for its staff in which they are provided with information about what PHI is, their obligations under *PHIPA*, their responsibilities in safeguarding and protecting PHI, and the consequences for failing to maintain confidentiality.

[74] The hospital confirmed that, starting in 2013 and on an annual basis thereafter, the radiologist was required to review the Confidentiality Policy and Privacy Policy, as well as sign a confidentiality agreement confirming that he completed the module of the Privacy and Confidentiality education program for Regulated Health Professionals.

[75] The hospital's staff is also required to complete an e-Health privacy and security module at the start of their employment for which they receive a certificate that is kept on file. They are also required to review the hospital's privacy policies and provide written confirmation that they have done so on an annual basis.

[76] Starting in the credentialing year 2022-2023 and going forward, the hospital advised that professional staff must also complete the Ontario Health training module "Privacy and Security Training for Health Care Providers Using the Provincial EHR" as part of their reappointment process. Once completed, the hospital advised that a certificate of successful completion must be obtained for the application to move forward through the credentialing process.

[77] As learning and a "cautionary tale" for all its staff, the hospital informed them of the disciplinary steps taken against the radiologist. The hospital also took steps to ensure that all professional staff are explicitly informed that name searches that result in patient PHI being accessed for any purpose other than providing patient care or carrying out their assigned duties, even without clicking into the record, is an unauthorized access.

Discipline

[78] To deter unauthorized accesses of PHI, custodians should have a discipline policy and related procedures in place.[18]

[79] In this matter, the disciplinary action was taken against the radiologist by the hospital in accordance with the hospital's privacy policies which included notifying the CPSO.

[80] However, the hospital also advised that the radiologist continues to hold privileges to provide on-call and after-hours outpatient health care to its patients. To provide this health care, the radiologist continues to have remote access to Cerner and AGFA PACS

[17] See footnote 7.
[18] See footnote 7.

through, and is authorized by the hospital to use, his radiologist home workstation.

[81] To prevent a similar breach by the radiologist, the hospital continues to audit his accesses to PHI in all health information systems that he has access to, including Cerner and AGFA PACS. The hospital plans to continue these audits and anticipates that the radiologist's accesses to PHI will be monitored for as long as he holds privileges.

[82] According to the hospital, there have been no unauthorized accesses by the radiologist since August 2021.

Analysis

[83] At issue is whether the hospital had reasonable measures in place at the time of the breach to ensure that the affected individuals' information was protected against unauthorized use.

[84] At that time, the hospital had privacy policies in place. These policies appear to be comprehensive and set out the expectations and obligations that the hospital had for its agents regarding the protection of PHI. They also appear to have been communicated by the hospital to its agents on an annual basis and specifically informed them that PHI must not be used without authorization. As evidence of this, the radiologist signed the hospital's confidentiality agreement each year in which he breached the privacy of the affected individuals. Further, the hospital also provided privacy training to staff informing them of their responsibilities to safeguard and protect PHI.

[85] But notably, the hospital only became aware of the radiologist's unauthorized uses of PHI after the sister-in-law made a privacy complaint to the local hospital. Since the breach was confirmed by audits of the radiologist's accesses in Cerner and the GE PACS, this raised questions about the ability of these systems to detect and deter unauthorized access to PHI.

[86] At the time of the breach, the hospital's ability to proactively detect unauthorized access to PHI in Cerner and the PACSs through audits was limited due to inherent system limitations that it appears the hospital could not unilaterally remedy as well as data processing challenges.

[87] To date, some of these deficiencies have not been resolved and, as a result, it may be possible for a similar breach to occur and go undetected until an affected patient raises a specific privacy concern to the hospital. Further, although these deficiencies did not hinder the hospital's ability to detect the radiologist's privacy breach on a reactive basis, there may be other circumstances in which they could do so.

[88] Moreover, as stated above, privacy notices and warning flags may serve to prevent or reduce the risk of unauthorized accesses to PHI. Particularly, a privacy warning flag can serve as an important deterrent to unauthorized access to PHI and assist in logging,

auditing and monitoring access with respect to EHR systems.[19] At the time of the breach, Cerner did not display a privacy notice or warning flag, and this may also have been the case for GE PACS.

[89] For these reasons, I do not find that the hospital had reasonable measures in place at the time of the breach to ensure that the affected individuals' information was protected against unauthorized use as required by section 12(1) of *PHIPA*.

[90] Despite this finding, I am encouraged by the remedial steps taken by the hospital to implement privacy warnings in Cerner and in AGFA PACS (for radiologists), and an auditing tool for name searches by users in AGFA PACS. These protective measures were not in place at the time of the breach.

[91] Further, with respect to the deficiencies in Cerner's auditing capabilities, this office has recognized that the duty in section 12(1) to take "reasonable" steps to ensure that PHI is protected does not require perfection and that there is nothing prescribed in *PHIPA* for what is reasonable. In addition, in the context of similar obligations on institutions under *FIPPA*[20] and *MFIPPA*[21], the IPC has explicitly recognized that a breach may occur where an institution had in place reasonable measures in compliance with its statutory obligations.[22] Accordingly, the requirement to take reasonable steps to protect PHI does not require a guarantee against snooping or other threats of unauthorized use of PHI.

[92] As such, it is important to note that even though Cerner is unable to proactively detect unauthorized access to PHI, it still gives the hospital the ability to conduct audits of PHI and the activities of their agents or users. In addition, Cerner also allows the hospital to respond to requests from patients or privacy complaints about who has used their PHI and provides analyzable data about the extent to which an agent or user has accessed patients' PHI within a given period. For these reasons, in my view, this EHR system still serves as a technical safeguard that can be used to deter and detect unauthorized use to PHI.

[93] Moreover, in response to the breach, the hospital identified the scope and took steps to contain it. The hospital also investigated the matter and took remedial steps that included highlighting to staff the disciplinary action taken against the radiologist to deter them from accessing patient (and their family's) PHI without authorization. Further, the hospital notified appropriate staff, all the affected individuals, the other regional hospitals that share Cerner and GE PACS, as well as the CPSO.

[94] In my view, the hospital's response appears to be in line with the recommended steps set out in the IPC's "Responding to a Health Privacy Breach: Guidelines for the

---

[19] See footnote 7.
[20] *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F.31.
[21] *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M.56.
[22] See PHIPA Decisions 44, 74, 82 and 124.

Health Sector".[23]

[95] Given the aforementioned, I am satisfied that the hospital has responded adequately to the breach and, therefore, find a review of this matter unnecessary.

Issue 2: Is a review warranted under Part IV of PHIPA?

[96] 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.

[97] In accordance with my delegated authority to determine whether a review is conducted under section 58(1) of *PHIPA*, and for the reasons set out above, I find that a review is not warranted.

NO REVIEW:

For the foregoing reasons, no review of this matter will be conducted under Part VI of the *PHIPA.*

Original Signed by: November 6, 2024

John Gayle
PHIPA Mediator/Investigator

[23] https://www.ipc.on.ca/en/resources-and-decisions/responding-health-privacy-breach-guidelines-health-sector