Information and Privacy Commissioner,
Ontario, Canada

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

PHIPA DECISION 70

HR16-177

A Long Term Care Home

February 20, 2018

Summary: A long term care home (the Home) contacted the Office of the Information and Privacy Commissioner of Ontario (the IPC) to report a privacy breach under the *Personal Health Information Protection Act, 2004* (the *Act*). This breach involved an employee who took two files containing the personal health information of two prospective residents home with her to review. On her way home, the employee lost the two files, which were never recovered. I conclude that the Home did not comply with section 12(1) of the *Act*, but find that in light of the Home's response to the breach and the improvements it has made since, no review will be conducted under Part VI of the *Act*.

Statutes considered: *Personal Health Information Protection Act, 2004*, sections 12(1) and 58(1).

Decisions considered: Orders HO-010 and HO-013; PHIPA Decision 64.

INTRODUCTION:

[1] This investigation was opened under the *Personal Health Information Protection Act, 2004* (the *Act*) as a result of information submitted by a long-term care home (the Home). The Home reported that files containing the personal health information of two individuals were lost by its employee.

BACKGROUND:

[2] On September 28, 2016, the Home contacted the Office of the Information and Privacy Commissioner of Ontario (the IPC) to report an incident involving personal health information. In its correspondence, the Home explained that "documents containing personal and medical information have been misplaced." The Home elaborated that, despite its efforts, it was unable to recover the files.

[3] As part of its "Privacy Breach Investigation Report" submitted to the IPC, the Home described the events of the breach, as well as its response. The Home explained that the incident occurred on the evening of September 6, 2016, when a staff social worker (the employee) removed two files containing the applications of two prospective residents to the Home when she left for the day. The employee travelled via public transit to a community centre to attend a class. Upon arrival at home that evening, the employee realized that she did not have the bag containing the two files. The employee reported the loss of the records to the Home the following morning.

[4] The information at issue consisted of two complete Community Care Access Centre (CCAC) files containing the medical and personal information of two potential residents. The files were provided via the CCAC's Resource Matching and Referral system, which is an electronic system used to securely transfer the files of applicant residents from the CCAC to the Home. It included names, addresses, medical diagnosis, medical history and the contact information of family members and treating physicians, as well as the health card number of each applicant resident.

[5] In conducting the investigation, I requested submissions from the Home. In response, the Home confirmed the information it provided in its initial report to the IPC. The Home described its response to the breach, including its efforts to locate the missing files, explaining that the employee retraced her steps to the community centre, public transit and the long-term care home. The Home made calls to the public transit authority's lost and found division but the files were never located.

[6] The Home advised that it notified both affected individuals, as it is required to do so under section 12(2) of the *Act*.

[7] The Home also informed the CCAC that the personal health information was compromised in case there are any inquiries related to the lost files.

[8] The Home identified the factors giving rise to the breach, describing it as an error in judgment by the employee. The Home explained that it does not permit staff to remove patient files from the facility. In explaining the decision to remove the files from the facility, the Home determined that the employee's workload issues and inexperience led her to take the files from the office to work on them at home. The Home explained that the employee did not consult with her supervisor to request permission to print and remove the patient files.

[9] In response to the breach, the Home undertook a number of steps, including meeting with the employee and providing time management training as well as retraining her on its privacy and business conduct policy, the confidentiality agreement and reviewing the privacy document contained in the employee's new hire package. The Home also revised their staff training.

[10] The Home amended its health care records policy to make it clear that staff cannot remove files from the facility unless prior arrangements have been made with the Administrator or if there is a subpoena. The Home explained that while staff do not need special permission to print information from the Resource Matching and Referral system, access is limited to social workers who are encouraged to only print when absolutely necessary.

DISCUSSION:

[11] There is no dispute that the Home is a "health information custodian" and that the records at issue contained "personal health information" under the *Act*.

[12] Based on the information set out above, as a preliminary matter, I find that the person who operates the Home is a "health information custodian" under paragraph 4.ii of section 3(1) of the *Act*, and that the records at issue are "personal health information" under sections 4(1)(a), (b), (d), (f) and (g) of the *Act,* which were in the custody or control of the Home. There is no dispute, and I further find, that the employee was an "agent" of the Home as that term is defined in section 2 of the *Act*.

ISSUE:

1. Did the Home take steps that were reasonable in the circumstances to protect personal health information in accordance with section 12(1) of the *Act*?

2. Is a review warranted under the *Act*?

RESULTS OF THE INVESTIGATION:

[13] In the circumstances under investigation, records of personal health information were lost and never recovered. Consequently, my investigation focussed on whether the Home took steps that were reasonable in the circumstances to ensure that personal health information in its custody or control was protected against loss.

1. Did the Home take steps that were reasonable in the circumstances to protect personal health information in accordance with section 12(1) of the *Act*?

[14] Section 12(1) of the *Act* requires that health information custodians take reasonable steps to ensure that records of personal health information in their custody or control are protected against loss, among other things. Specifically, section 12(1) 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.

[15] At the time of the breach, the Home's policies and procedures did not explicitly prohibit the removal of files containing personal health information from the facility. As such, the employee did not appear to be aware that the removal of the files was prohibited or otherwise required permission from senior staff. The lack of clarity, combined with other factors identified by the Home such as workload and employee inexperience, resulted in the files being handled in an insecure manner and subsequently lost.

[16] In Orders HO-010 and HO-013, and more recently PHIPA Decision 64, the IPC considered "reasonable" for the purposes of section 12(1) of the *Act*, to include a health information custodian reviewing its measures to protect personal health information. Health information custodians are expected to identify risks to privacy and take reasonable measures to reduce or eliminate such risks and mitigate the potential harms that may arise.

[17] To assist health information custodians in understanding and meeting their obligation to protect personal information, the IPC has published guidelines that address privacy breaches in the health sector. The IPC's "What to do When Faced With a Privacy Breach: Guidelines for the Health Sector" informs health information custodians how to prepare and respond to breaches, as well as how to minimize the chances of a privacy breach occurring.[1] This includes having privacy policies, implementing privacy education and training programs as well as having a privacy breach protocol in order to quickly respond to privacy breaches.

[18] The Home's administrative safeguards were particularly relevant to my investigation into these lost records, and I highlight the following.

---

[1] https://www.ipc.on.ca/wp-content/uploads/Resources/hprivbreach-e.pdf

Administrative Measures or Safeguards

Privacy Policies & Procedures

[19] The Home has a "Resident Care Manual", a human resources "Administration Manual" and a "Breach of Privacy" guideline document. The Home's "Resident Care Manual" sets out guidelines for the disclosure, transfer, retention and destruction of records, while the "Administration Manual" addresses privacy and confidentiality. Prior to the breach, the Home's policy did not explicitly prohibit the removal of health records from the facility.

[20] The Home's Breach of Privacy guideline is a comprehensive document that defines "personal health information" and "privacy breach" and provides direction for staff when a privacy breach occurs.

[21] The Breach of Privacy guideline includes, among other things, the following requirements:

1. All staff must report suspected or actual breach of privacy to the Administrator/Director of Care/Designate.

2. Upon being informed of a suspected or actual privacy breach, the Administrator/Director of Care/Designate includes the following breach management requirements:

    - Contain the breach as required, including revoking access to computer systems and stopping unauthorised activities;

    - Initiating an investigation to identify the personal health information involved, the cause and extent of the breach, the affected individual and foreseeable harm;

    - To produce a privacy breach investigation report;

    - Notify affected individuals;

    - Identifying and contacting external groups that may need to be notified of the breach, such as privacy commissioners, the police and regulatory bodies;

    - Evaluate the causes of the breach and implement plans to prevent future privacy breaches; and

    - Educate staff regarding the privacy breach.

[22] In the circumstances under investigation, the Home implemented its protocol once the breach was reported. It undertook efforts to contain the breach, although

these were ultimately unsuccessful as the records could not be located. The affected individuals were notified of the breach and the Home followed up with an internal investigation that included meeting and working with the employee to both identify and review the circumstances surrounding the breach and the adequacy of existing privacy policies and procedures.

[23] In response to the breach, the Home informed the IPC that it revised its "Resident's Care Manual" to make it clear that staff cannot remove files from the facility. The Home stated that either the Executive Director or Director of Care will assist staff in accessing patient files to ensure that documents are not printed unnecessarily and that they remain in the facility.

Confidentiality Agreements

[24] All of the Home's staff sign a "Standards of Employee Conduct", including a "Pledge of Confidentiality" upon hire and sign again annually.

[25] The Home's "Standards of Employee Conduct" requires staff to respect residents' privacy and to maintain confidentiality of the information obtained during their employment. Staff must confirm that they have read, understand and will comply with the "Standards of Employee Conduct", as well as additional policies of the Home. The Home requires the Administrator/Department Head to review the importance of confidentiality with new staff during orientation as well as annually during performance appraisal or in-service.

Privacy Training and Education

[26] The Home informed the IPC that privacy training is provided as part of the Home's orientation of new staff as well as through mandatory annual privacy education. The Home explained that all of its staff participate in mandatory privacy training and that the training is offered electronically and completion is tracked. The Home offers in-class training sessions and explained that a copy of a document titled "Confidentiality and Privacy" is placed on each unit for staff to read. In addition, since the breach, the Home's privacy training material has been revised to explicitly instruct staff that personal health information shall not be removed from the facility.

[27] The Home described its efforts to work with the employee to address issues giving rise to the breach. Prior to the incident giving rise to the breach, the Home provided the employee with privacy training. The employee had signed the "Pledge of Confidentiality" describe above. As well, the employee was trained on the CCAC's Resource Matching and Referral system, which included information on confidentiality and security.

[28] In response to the breach, the Home undertook a number of steps. As previously described, they met with the employee and provided her with additional refresher training. The employee also assisted with revising the privacy posters that are placed at

each nursing station and the main bulletin board located at the entrance to the Home's facility. In addition, the employee assisted with gathering information and preparing letters and follow up to mitigate the risks related to the breach. The employee also gave an in-service presentation to fellow staff on the potential risks to residents' privacy. The Home explained that the employee's participation in these exercises was undertaken to assist her to learn about the consequences of her actions.

[29] While the Home stated it did not permit staff to remove patient files from the facility, its written policies did not address this and staff were inadequately trained on this policy. Whether this shortfall, in itself, meant that the Home did not comply with section 12(1) of the *Act* at the time of the breach, I am satisfied that it has since addressed the issue.

[30] I have considered the above described policies and practices, the circumstances of this particular breach, the Home's response to the breach and the improvements since that time and I conclude that no review is necessary.

2. Is a Review Warranted under the *Act*?

[31] 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.

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

DECISION:

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

Original Signed by: February 20, 2018

Jeffrey Cutler
Investigator