MANITOBA OMBUDSMAN

THE PERSONAL HEATH INFORMATION ACT INVESTIGATION REPORT

Southern Health-
Santé Sud

Privacy Breach:
Use, Disclosure
and Security of
Information

CASE# MO-01541/2020-0251
Public Report with Recommendations

Issue Date:
December 2024

Provisions considered:
PHIA – 5(1), 6(2), 13(1), 13(2), 16, 18(1), 18(2), 20(1), 20(2), 20(3), 57, 63(2)(a), 63(2)(b), 63(3)(a)
PHIA Regulation – 2, 3, 4(1), 4(4), 5, 6, 8(1), 8(2)

SUMMARY

In March of 2020, Southern Health-Sante Sud Regional Health Authority (the RHA) became aware of a privacy breach where a privacy officer was accessing personal health information (PHI) of a third party without authorization. The RHA regional privacy officer reported the privacy breach to our office, and we also received complaints from two individuals who alleged that their PHI was accessed inappropriately.

Our office investigated the complaints and determined that the use of the complainants' PHI was not authorized. Our office also reviewed policies, procedures and other information provided by the RHA and found that it had not met the security requirements and standards for the protection of personal health information set out under The Personal Health Information Act. Our office is therefore making recommendations to the RHA to address the issues identified during our investigation.

TABLE OF CONTENTS

INTRODUCTION

This report concerns an investigation under *The Personal Health Information Act* (PHIA), relating to the unauthorized access of PHI of third parties by a privacy officer at a healthcare the facility (the facility). The facility is operated and staffed by the RHA. Our office determined that, as the facility is not a separate entity and is staffed by RHA employees, the RHA is the trustee under PHIA.

PHI is some of the most sensitive information available about an individual. The public must have confidence that trustees are not misusing or otherwise putting their PHI at risk.

The lack of confidence in the security of their PHI can lead the public to refuse to allow trustees to collect or use their PHI. It can also result in members of the public refusing or delaying medical appointments out of concern for the risk to the security of their PHI. When the public loses confidence in the health care system's ability to protect their PHI, they can also lose confidence in the health care system as a whole.

Relevant Acronyms:

- PHIA = The Personal Health Information Act
- PHI = personal health information
- EPR = electronic patient record
- RoUA = Record of User Activity

Relevant Parties

- Southern Health-Santé Sud Regional Health Authority (the RHA)
- Southern Health-Santé Sud Privacy Officer (RHA PO)
- The healthcare the facility (the facility)
- The healthcare the facility Privacy Officer (the facility PO)
- Individuals whose PHI was accessed (the individuals)

BACKGROUND

On April 23, 2020, the RHA notified our office that an individual's privacy had been breached. Shortly thereafter, our office received two complaints related to this matter. Three individuals also made privacy complaints to the RHA related to the use of their PHI. These complaints were investigated by the RHA PO.

Our office opened three investigations, an OOI[1] under Part 4 of PHIA and two complaint investigations under Part 5. We issued separate reports for the two complaint investigations and in those reports, we found privacy breaches of both individuals' PHI.

The OOI investigation was opened to look at the circumstances of the breaches, the steps the RHA took to address the breaches, and any measures taken by the RHA to limit the risk of further breaches. Specifically, we sought to review the policies, procedures, and security safeguards of the RHA. This is the report for the OOI investigation.

The RHA's Privacy Breach Investigations

In response to the privacy complaints, the RHA PO conducted an audit of the Electronic Patient Records for the individuals. The audits confirmed that the facility PO had accessed the individuals' PHI. The RHA PO opened privacy breach investigations into these accesses.

The RHA determined for one of complaints that the access of the individual's PHI was authorized due to the timing of the access and the pattern of the other accesses by the facility PO at that time. For another individual, the facility PO admitted to accessing the individual's PHI inappropriately. Based on this admission, the RHA determined that a privacy breach occurred.

For the last individual, the RHA was unable to find conclusive evidence as to whether the access was authorized or not. The RHA ultimately decided that the use of the individual's PHI was authorized, and no breach occurred.

[1] An OOI or Ombudsman's Own Investigation is an investigation undertaken at the Ombudsman's discretion under clause 28(a) of PHIA. These investigations do not require a complaint and are done to monitor and ensure compliance with the requirements of PHIA.

The RHA notified the individuals of its findings and of their right to make a complaint to the Ombudsman.

The RHA also notified our office of the breach of the one individual's PHI. At the time this breach occurred, reporting privacy breaches to the Ombudsman was considered a best practice under PHIA, but was not required[2].

Our Office's Complaint Investigations and Prosecution

We completed our investigation of the two complaints regarding access to individuals' PHI in January of 2021. For one individual, the RHA determined that a privacy breach occurred. Our office came to the same conclusion and determined that the use of the individual's PHI was unauthorized.

As mentioned above, the RHA was unable to find conclusive evidence as to whether the access was authorized and determined that no breach occurred. The RHA based its conclusion on the absence of evidence that the use of the individual's PHI was unauthorized. It is our office's view that trustees must demonstrate positive evidence that their use of an individual's PHI is authorized.

In the absence of such evidence, the use must be considered unauthorized under PHIA. As such, our office found that the use of the individual's PHI was not authorized.

Prosecution

Based on the evidence gathered during our investigation, Manitoba Prosecution Service (Prosecutions) determined that there was sufficient evidence to proceed with an offence prosecution in relation to the breach of an individual's PHI.

On June 28, 2021, the Ombudsman filed three charges against the facility PO under clauses 63(2)(a), 63(2)(b) and 63(3)(a) of PHIA.

[2] In 2022, amendments to PHIA came into force and subsection 19.0.1(2) required trustees to notify affected individuals and to report breaches to the Ombudsman where there is a real risk of significant harm.

Offence by employee, officer or agent

63(2) *Despite subsection 61(2), a person who is an employee, officer or agent of a trustee, information manager or health research organization and who, without the authorization of the trustee, information manager or health research organization, wilfully*

(a) discloses personal health information in circumstances where the trustee, information manager or health research organization would not be permitted to disclose the information under this Act; or

(b) uses, gains access to or attempts to gain access to another person's personal health information;

is guilty of an offence.

Offences by trustees and information managers

63(3) *A trustee, information manager or health research organization who*

(a) collects, uses, sells or discloses personal health information contrary to this Act;

is guilty of an offence.

On July 7, 2022, the facility PO pleaded guilty to the charge of unauthorized use of PHI under clause 63(2)(b) of PHIA and received a fine of $5500.00.

Our office does not issue investigation reports related to a prosecution until after the prosecution has been completed. During this time, the OOI investigation was also paused so that all matters related to the prosecution could be completed. While the investigations and the issuing of reports were paused, our office provided updates on the prosecution to the parties involved.

We also sought and received updates on steps taken by the RHA to improve its privacy program during this period. On November 10, 2022, we issued the final investigation reports related to the two complaints we received.

PART 4 INVESTIGATION

As previously noted, our office also initiated an investigation under part 4 of PHIA to review the RHA's compliance with PHIA. The purpose of this type of investigation is to ensure that the trustee has dealt with the privacy breach effectively and to ensure the trustee's policies, procedures, and practices sufficiently reduce the risk of further unauthorized access to PHI and meet the requirements of PHIA.

Our office requested copies of the RHA's policies and procedures for privacy breaches, audits, and any other polices related to PHIA. We also reviewed the RHA's audits of user activity conducted on the facility PO's access of the individuals' PHI.

Our office would consider this privacy breach to be significant as the individual who made unauthorized access of PHI was the privacy officer for the facility. The facility PO was also an Information Manager, meaning that they were responsible for ensuring that the information kept in the information management systems was accurate.

The facility PO had access to the information at the facility and access to the RHA's systems, including access to the patient records for anyone who attended an RHA the facility. Section 57 of PHIA sets out the duties of a privacy officer:

> ***Privacy officer for the facility and agency***
> ***57*** *A health care the facility and a health services agency shall designate one or more of its employees as a privacy officer whose responsibilities include*
>
> *(a) dealing with requests from individuals who wish to examine and copy or to correct personal health information under this Act; and*
>
> *(b) generally facilitating the trustee's compliance with this Act.*

Facilitating a trustee's compliance with the Act can include ensuring that the policies and procedures of the trustee comply with PHIA, ensuring that employees receive training on PHIA, investigating any privacy complaints, and ensuring that the PHI in the care and control of the trustee is protected and used appropriately.

When the person responsible for ensuring the correct use of PHI misuses that information, the result is a significant breach of trust not only for the individual whose

privacy was breached but for the community as a whole. Breaches of this kind affect how community members feel about the protection and privacy of their PHI and how they interact with the healthcare system.

During this investigation, our office identified concerns relating to how the breach was addressed by the RHA as well as the measures in place to prevent a similar situation from occurring in the future.

We set out and discuss each of the issues below.

1. Documentation of Audit Activities

Regular audits of access to PHI support transparency and accountability in the use of PHI, which enhances public trust and confidence in the healthcare system's ability to manage PHI and protect privacy.

Legislative Requirements

The *Personal Health Information Regulation* (the regulation) sets out requirements for trustees to ensure the security of PHI and to audit their security safeguards. There are also requirements that trustees have written security policies and procedures and that they audit records of user activity.

> ***Written security policy and procedures***
> ***2*** *A trustee shall establish and comply with a written policy and procedures containing the following:*
>
> *(a) provisions for the security of personal health information during its collection, use, disclosure, storage, and destruction, including measures*
>
> *(i) to ensure the security of the personal health information when a record of the information is removed from a secure designated area, and*
>
> *(ii) to ensure the security of personal health information in electronic form when the computer hardware or removable electronic*

storage media on which it has been recorded is being disposed of or used for another purpose;

(b) provisions for the recording of security breaches;

(c) corrective procedures to address security breaches.

Additional safeguards for electronic health information systems

4(1) *In accordance with guidelines set by the minister, a trustee shall create and maintain, or have created and maintained, a record of user activity for any electronic information system it uses to maintain personal health information.*

4(4) *A trustee shall audit records of user activity to detect security breaches, in accordance with guidelines set by the minister.*

Audit

8(1) *A trustee shall conduct an audit of its security safeguards at least every two years.*

8(2) *If an audit identifies deficiencies in the trustee's security safeguards, the trustee shall take steps to correct the deficiencies as soon as practicable.*

PHIA also requires trustees to ensure that the PHI used or disclosed by a trustee is accurate, up to date, complete and not misleading:

Duty to ensure accuracy of information

16 *Before using or disclosing personal health information, a trustee shall take reasonable steps to ensure that the information is accurate, up to date, complete and not misleading.*

PHIA requires trustees to adopt security safeguards to protect the personal information they collect. Part of this responsibility is ensuring that only those who have a right to access PHI are doing so. These requirements are set out below.

Duty to adopt security safeguards

18(1) *In accordance with any requirements of the regulations, a trustee shall protect personal health information by adopting reasonable administrative,*

technical and physical safeguards that ensure the confidentiality, security, accuracy and integrity of the information.

Specific safeguards
18(2) *Without limiting subsection (1), a trustee shall*

(a) implement controls that limit the persons who may use personal health information maintained by the trustee to those specifically authorized by the trustee to do so;

(b) implement controls to ensure that personal health information maintained by the trustee cannot be used unless

(i) the identity of the person seeking to use the information is verified as a person the trustee has authorized to use it, and

(ii) the proposed use is verified as being authorized under this Act;

(c) if the trustee uses electronic means to request disclosure of personal health information or to respond to requests for disclosure, implement procedures to prevent the interception of the information by unauthorized persons; and

(d) when responding to requests for disclosure of personal health information, ensure that the request contains sufficient detail to uniquely identify the individual the information is about.

The purpose of these sections of PHIA and the regulation are to ensure that PHI is only accessed for an authorized purpose by an authorized person and that the PHI is correct and up to date. Privacy-related audits of electronic systems help trustees know when, how and by whom PHI is used.

Documenting those audits allows trustees to identify regular patterns of access and detect patterns that indicate potentially inappropriate access. Such documentation also creates a record of why PHI was accessed during the audit. Quality-assurance audits help trustees ensure that the information is correct and up to date.

The Minister of Health has established a set of guidelines for Records of User Activity (RoUAs) which include guidelines for conducting privacy-related audits of systems that contain PHI, as required by subsection 4(4) of the regulation.
The guidelines require trustees to have a process for how privacy-related audits are completed. In addition, they require trustees to have a process for checking the checker. I.e., ensuring that accesses by those employees tasked with auditing the systems and actions of other employees are also reviewed to ensure that they are using PHI appropriately.

The guidelines also set out the several types of privacy-related audits that should be done. Random audits occur at random intervals as set out by the trustee. These audits can be set up to identify specific triggers, such as when an employee accesses the PHI of someone with the same last name or an individual who has appeared in the media. There are also focused audits that are conducted when the trustee identifies a specific issue that needs to be investigated, such as when a complaint of unauthorized use is made.

PHIA, the regulation, and the guidelines all require trustees to ensure that systems containing PHI are being audited and that the trustee has a set process for how that occurs.

Any auditing process established by a trustee should include requirements for how users are selected for an audit, how often an audit is conducted, what types of accesses are searched for, what happens if a suspicious access is found, a way to record that the audit was conducted, and the outcome of the audit.

Audit Information Provided by the RHA

The RHA indicated that privacy-related audits are conducted by RHA and/or at the facility level, in this case it would be the facility. There are several types of audits that may involve viewing patient PHI in electronic systems. Some of these audits (as required under PHIA) can occur at random or in response to a complaint. Other audits are done for quality assurance purposes such as an audit for the purpose of balancing month end statistical information or to ensure that the information in patient files, such as the address of a doctor, is correct.

The RHA PO indicated that quality assurance audits generally happen at a certain time of year, so if patient files are accessed during these periods, it is assumed that the accesses are for that purpose. For these audits, files can be pulled at random or, if there is specific information that needs updating, specific files are reviewed.

Our office asked the RHA how files are chosen for the privacy-related audits. The RHA indicated that there are several electronic health information systems used within healthcare and each system has different methods for conducting privacy-related audits.

The main systems used by the RHA are eChart, the Electronic Patient Record (EPR) and the Electronic Medical Record (EMR). Shared Health, which is the trustee for the PHI in e-Chart and an information manager (IT solution provider) for the EPR system, conducts user-centric audits of these systems every one to two years. Shared Health will also run 'same name'[3] audits on these systems at random intervals.

The EMR system is maintained by the RHA. There are two other systems that can be accessed by employees of the RHA. They are the Public Health Information Management System (PHIMS) and Procura. Like eChart and EPR, the RHA does not initiate the audits for these systems but participates in Shared Health's audit activities.

Our office requested copies of any RHA policies related to audits. The RHA provided one such policy, which requires an audit of security safeguards to be done every two years. While there is no policy requiring other audits be done, the RHA PO began running same name audits in the EMR system in 2022.

The RHA PO indicated that they would request a report of user activity in EPR and eChart from Shared Health | Digital Health regarding access to PHI on persons of interest (for example, someone in the news) or where there is a suspicion an employee's access or activities may be in contravention of PHIA. The RHA can also request an audit of user activity in the other systems if required.

[3] A 'same name' audit refers to process of identifying individuals within a database who share the same name. One of the key aspects of this audit is ensuring that the correct individual is associated with their specific data and access history, even if others share their name.

The RHA PO keeps a spreadsheet of all the privacy-related audits that they are aware of. They also log all suspected/real breaches or complaints about potential breaches. Each log is hyper linked to a file folder.

The spreadsheet tracks three types of audits: same name audits, special request audits (those requested when there is a specific concern about an employee's access) and random record of user activity audits. However, the spreadsheet does not include audits done for other purposes, such as quality assurance, or audits done on other systems.

Analysis

When the RHA was investigating the privacy breaches of the PHI of the individuals, they determined that one individual's information was likely accessed as part of an audit of user activity by the facility PO and their access for an audit purpose would be authorized. The RHA could not determine whether there was an audit that involved accessing another individual's PHI.

The RHA's policies and procedures do not document the details of the auditing process for privacy-related audits as required in the guidelines established by the regulation nor do they have a requirement for records of the audits to be kept.

Creating a log of audits of user activity helps trustees demonstrate that they complied with the requirements of PHIA, the regulation, and the guidelines. While not required by PHIA, having a log of audits done for quality assurance purposes would also document that PHI was accessed for quality assurance purposes. This would in turn help the trustee verify and demonstrate both the identity of the person making the access and the purpose and the authority for that access, which is required under clause 18(2)(b) of PHIA.

Subsection 2(b) of the regulation requires trustees to have policies and procedures with provisions for the recording of security breaches. Creating a log of all suspected breaches helps trustees meet this requirement and promotes compliance with the requirements under PHIA related to privacy breach risk assessments, notifying affected

individuals, and reporting privacy breaches to our office, when they are assessed as likely to cause a real risk of significant harm to the individual[4].

The RHA PO's informal process to track privacy-related audits received from Shared Health | Digital Health is a good first step, but the lack of a written policy or procedure requiring that privacy-related audits be tracked means that many privacy-related audits were not tracked or otherwise documented at the time of the breaches. Quality assurance audits, which make up a sizable portion of the total audits conducted by the trustee, are not tracked at all.

The absence of tracking and documentation on quality assurance audits meant that although the accesses of the individuals' PHI were believed to be linked to a quality assurance audit purpose, there was no direct evidence that the use of their PHI was authorized. The RHA determined that the accesses were authorized because of the time of year and the lack of any evidence that the accesses were unauthorized.

This is not sufficient under PHIA. Sections of both PHIA and the regulation require trustees to have policies and procedures related to the security of information and it is incumbent on trustees to ensure that PHI is used only when authorized. In a situation where the trustee is unable to determine whether the use was authorized, the trustee should not default to considering the access/use to be authorized.

The RHA should use situations like this to review its policies, procedures, and training to remove any gaps that exist and make any necessary changes, especially those that would allow for the RHA to determine more accurately in the future whether an access was authorized.

Citizens have a right to know when and how their PHI is used, and trustees should take any opportunity they can to ensure that they are able to provide this information to individuals who have questions or concerns about access to their PHI.

The lack of a requirement to track or otherwise document audits or other accesses of PHI where there would be little to no corroborating evidence (as opposed to medical notes or billing records where situational evidence would exist) means that the RHA is unable

[4] As noted above, the requirement to notify affected individuals and our office was added to PHIA after this investigation began but is a requirement now.

to adequately determine whether an access was authorized. This could lead to a situation where, as it did in this case, an individual no longer trusts that the RHA can protect their privacy and the security of their PHI.

Our office finds that the RHA did not fully meet the requirements of PHIA, the regulation, and the guidelines by failing to have a policy and process for conducting audits and documenting the audits conducted by the RHA.

2. Lack of Compliance with the RHA Policy Related to Confidentiality of PHI

The facility PO accessed the PHI of an individual, when there was a potential for a conflict of interest, and the RHA determined this access was authorized because the access occurred at a time when audits generally took place and there were other accesses by the facility PO that were consistent with this conclusion. The ability of any organization to recognize a potential conflict of interest and address it appropriately can significantly affect the level of trust citizens have in that organization.

This is critically importance for healthcare organizations who handle PHI. The more sensitive the information is, the greater the potential effect that a conflict of interest can have on an individual. And PHI is some of the most sensitive information that exists.

Legislative Requirements

PHIA requires trustees to implement controls for who can access PHI maintained by the trustee:

> ***Specific safeguards***
> ***18(2)*** *Without limiting subsection (1), a trustee shall*
>
> *(a) implement controls that limit the persons who may use personal health information maintained by the trustee to those specifically authorized by the trustee to do so;*
>
> *(b) implement controls to ensure that personal health information maintained by the trustee cannot be used unless*

(i) the identity of the person seeking to use the information is verified as a person the trustee has authorized to use it, and

(ii) the proposed use is verified as being authorized under this Act;

PHIA also requires trustees to limit their employees' use of PHI to the minimum amount necessary to accomplish a purpose authorized by PHIA:

Limit on the trustee's employees

20(3) *A trustee shall limit the use of personal health information it maintains to those of its employees and agents who need to know the information to carry out the purpose for which the information was collected or received or to carry out a purpose authorized under section 21.*

The regulations require a trustee to determine the PHI each of its employees is authorized to access:

Authorized access for employees and agents

5 *A trustee shall, for each of its employees and agents, determine the personal health information that he or she is authorized to access.*

The guidelines also include requirements for trustees to have policies and procedures in place to ensure that the requirements of PHIA are complied with.

RHA Policy Requirements

The trustee provided a copy of its policy on the Confidentiality of Personal Health Information, which includes the following:

- **Staff are not permitted to access confidential information about themselves, their family, friends or co-workers** *without following the access to information procedures set out in the Southern Health-Santé Sud policy.*

- **Staff who,** *in the performance of their duties,* **are required to have access to confidential information** *about* **a family member, friend or co-worker will:**

- **consult with their manager** *to determine if another staff member should be assigned, where possible; and*

- **where required and practical, obtain verbal consent** *from the client prior to fulfilling these duties.*

Emphasis added.

Analysis

Our office found no direct evidence that the access of the individual's PHI was part of an audit. There was also no evidence that the facility PO consulted with their manager prior to accessing the individual's PHI, as required by the policy.

The RHA also did not provide any information about whether the facility PO discussed this with their manager (RHA PO, or CEO) or obtained the individual's consent prior to accessing their PHI. The RHA's investigation also did not indicate whether it considered the requirements of this policy when making its decision.

The policy is straightforward and requires that an employee consult with their manager and obtain consent where required and practical before accessing the PHI of a family member, friend or co-worker.

Employees are generally not authorized to access the PHI of their family, friends, and co-workers because of the potential for perceived or actual conflict of interest. Consultations with managers and obtaining the consent of the individual are done to help address the concerns a perceived conflict of interest can raise.

An employee's authority to access PHI under PHIA flows from the job responsibilities and functions assigned to them by the trustee. Trustees may further restrict each employee's access to PHI, by means of technical, administrative, and physical safeguards.

PHIA and the regulation require trustees to limit the access their employees have to PHI to only what is necessary. Limits to access can include restricting access to certain types of information or systems only to specific roles or individuals, which is a technical safeguard. Other limits may be set by policy (an administrative safeguard), such as the limit on access to the PHI of people known to the employee.

The RHA set a limit on the ability of its employees to access PHI when the PHI is that of the employee, their family, friend, or a co-worker unless specific steps are taken. Any access of the PHI of friends, family, and co-workers where the required steps were not completed is not authorized by the Trustee. All access that is not authorized by the Trustee is not authorized by PHIA.

If the facility PO was conducting an authorized audit when they accessed the individual's PHI, then they should have consulted with their manager or obtained the individual's consent, as required. Per RHA policy, failure to take either of these steps means that the facility PO was not authorized to access the individual's PHI.

As there is no evidence that either of these steps were taken by the facility PO, the access of the individual's PHI was not authorized. Therefore, our office finds that the individual's privacy was breached.

Our office also finds that the RHA failed to comply with its own policy related to the use of PHI. Ultimately, this is a breach of the requirements under PHIA and the regulation to ensure that PHI is used only as authorized and limited to only those who need to know the information.

3. Lack of Communication Between Different Roles/Areas Within the RHA

For one individual, the RHA was aware of issues in the relationship between that individual and the facility PO and that a complaint was made by the individual. Ideally, a complaint about an employee whose role (both as a privacy officer and an information manager) provides them with greater access to PHI should have raised the potential for privacy concerns with the RHA.

However, in this case, the potential risk to privacy was not identified nor was the RHA PO made aware of the complaint. The lack of identification of the risk resulted in lack of communication between different functional areas within the RHA. As a result, the RHA PO was not able to appropriately consider whether the validity or motivation of the facility PO's access of the individuals' PHI in their investigation.

Legislative Requirements

PHIA requires trustees to protect PHI by adopting administrative, technical, and physical safeguards:

> ***Duty to adopt security safeguards***
>
> ***18(1)*** *In accordance with any requirements of the regulations, a trustee shall protect personal health information by adopting reasonable administrative, technical and physical safeguards that ensure the confidentiality, security, accuracy and integrity of the information.*

These safeguards would include ensuring that all employees of the trustee receive sufficient training to know what information they can access, when they can access it and how to recognize when access to information is unauthorized or there is a risk that the security of the information might be breached.

The regulation requires trustees to provide training to their employees:

> ***Orientation and training for employees***
>
> ***6*** *A trustee shall provide orientation and ongoing training for its employees and agents about the trustee's policy and procedures referred to in section 2.*

RHA Policy Requirements

The RHA's Reporting and Investigating Privacy Breaches and Complaints policy contains the following requirements:

> *The appropriate resources, including Human Resources, the Privacy and Access Specialist or Quality, Patient Safety and Accreditation should be consulted prior to interviewing Staff where education and/or corrective action may be required.*
>
> *If it is determined that a Privacy Breach has occurred, the manager shall consult with Human Resources and the Privacy and Access Specialist to establish the appropriate level of education and/or corrective action to be applied.*

The Confidentiality of Personal Health Information Policy requires all employees of the RHA to protect confidential information, including PHI. This policy includes the following requirements:

- *Staff are obligated to protect confidential information as outlined below and understand this obligation continues after their employment/contract/association/appointment with Southern Health-Santé Sud ends.*

- *All employees and Persons Associated with the Trustee are responsible for protecting all Personal Health Information including Demographic Information (oral or Recorded in any form,) that is obtained, handled, learned, heard or viewed in the course of his/her work or association with the Trustee.*
- *Staff have a legal, professional and ethical responsibility to protect all confidential information (oral or recorded in any form) that is obtained, handled, learned, heard or viewed in the course of their work or association with Southern Health-Santé Sud.*

Analysis

PHIA requires all employees of a trustee to be aware of the requirements of PHIA. For there to be meaningful compliance with PHIA, employees must be able to understand when they are authorized to access PHI and when access is not authorized. Employees must also be able to recognize the potential risks to privacy that can arise as part of their duties, including their oversight of others' duties.

The RHA policy requires the various program areas to be informed of and involved in investigations and outcomes related to privacy breaches. However, this should also apply in the reverse so that program areas must inform the privacy officer when a risk to privacy is created or identified.

In this situation, there was a specific complaint about an employee, who had access to a significant amount of personal information. Based on the employee's position and the nature of the complaint, employees of the RHA should have recognized the potential privacy implications and should have then consulted with the RHA PO.

Had the RHA PO known about the complaint, this may have changed the outcome of the RHA's investigation into the access of the individuals' PHI and may have caused the RHA to implement measures to prevent future access to the PHI by the facility PO.

Our office finds that the RHA was not compliant with PHIA and its regulations by not identifying the potential risk to the security of PHI and not providing sufficient training to its employees to enable them to identify that risk

4. The RHA's Handling of Privacy Breach Complaints

PHIA requires trustees and their employees not to use or disclose PHI except as authorized and to only use the minimum amount necessary to accomplish their purpose. Section 18 of PHIA requires trustees to have security safeguards for PHI and section 20 states that trustees "shall not use or disclose personal health information except as authorized".
The use of the word "shall" in PHIA shows a clear intention to place specific requirements on trustees. PHIA does not place any such requirements on individuals.

Placing the onus of proving that a use of PHI was unauthorized on the individual can also have a negative effect on the trust the individual has in the trustee, and on the healthcare system as a whole, and its ability to protect their PHI.

Trustees have a responsibility to ensure that PHI is being used as authorized under PHIA and trustees should bear the burden of proving that the use was authorized. That burden should not be placed on the person whose rights were potentially infringed upon.

Legislative Requirements

Duty to adopt security safeguards

18(1) *In accordance with any requirements of the regulations, a trustee shall protect personal health information by adopting reasonable administrative, technical and physical safeguards that ensure the confidentiality, security, accuracy and integrity of the information.*

General duty of trustees re use and disclosure

20(1) *A trustee shall not use or disclose personal health information except as authorized under this Division.*

Limit on amount of information used or disclosed

20(2) *Every use and disclosure by a trustee of personal health information must be limited to the minimum amount of information necessary to accomplish the purpose for which it is used or disclosed.*

Limit on the trustee's employees

20(3) *A trustee shall limit the use of personal health information it maintains to those of its employees and agents who need to know the information to carry out the purpose for which the information was collected or received or to carry out a purpose authorized under section 21.*

Information Provided by the RHA

The RHA indicated that it investigated the alleged privacy breaches of the PHI of the individuals. In one individual's case, the RHA did not find any evidence that the accesses were unauthorized. It determined that the access of one individual's PHI occurred during the time of year when a quality-assurance audit would take place, and the PHI of other individuals was accessed.

The RHA found no evidence one way or the other related to the second individual. The access of the individual's PHI did not occur during a specific time of year, was not done at the same time as the access of the PHI of others and there was no indication that a random audit was being done.

The RHA found that the access of both individuals' PHI was authorized. The RHA indicated that this decision was made on the understanding that, if there is no direct evidence of unauthorized access or bad behavior (such as an admission of guilt by the facility PO.), then the access must be considered authorized.

Analysis

In a situation where there is no information about the purpose for the access, trustees should not default to considering the access/use to be authorized. Subsection 20(1) of PHIA states that a trustee "*shall not use or disclose personal health information except as authorized*" and sections 21 through 24 list the specific situations where trustees are authorized to use (s. 21) or disclose (s. 22, 23, and 24) PHI. Any use or disclosure not indicated in those sections is not authorized under PHIA.

Trustees have the onus of demonstrating that their access to PHI is authorized under PHIA. When the RHA PO reviewed the privacy breach complaints, this onus was shifted to the individuals, meaning that they assumed the access was authorized unless the individuals could prove otherwise.

Our office explained to the RHA that this is not the correct way to determine whether an access was authorized under PHIA. The RHA PO indicated that they understood and would adjust how they investigated privacy breaches in the future.

Our office found that the use of one individual's PHI was not authorized because the facility PO did not follow RHA policy requirements that would have applied if the access truly was for a work-related purpose.
The facility PO did not obtain the individual's consent before using their PHI and there is no record of the facility PO ever meeting with their manager to discuss the potential conflict of interest as required by RHA policy.

There was also no direct evidence that the access was done for an authorized purpose. The only evidence that this access may have been part of an audit was the time of year it occurred and the access of other individuals' PHI at around the same time.

Our office found that the access of the other individual's PHI was not authorized because there was no evidence of the purpose for accessing the information. There was also no circumstantial evidence that the access may have been part of an audit or another legitimate purpose.

PHIA requires trustees to ensure their employees only access PHI when they have an authorized purpose. This means that a trustee must know the purpose for their employees' access of PHI. The burden is on the trustee to ensure that access/use by its employees is authorized and that only the minimum amount of information necessary for the purpose was accessed/used.

A situation where there is no way to determine whether an access was authorized should cause the trustee to review its policies, guidance, assignment of user access privileges, training and any other relevant information to ensure employees clearly understand what constitutes authorized access for their roles, and to identify any changes that need to be made to ensure that identifying authorized accesses is easier in the future.

PHIA also requires trustees to have reasonable administrative safeguards, which would include investigating privacy breaches and sufficiently identifying privacy risks. When a trustee shifts the onus to a complainant in a privacy breach investigation, the trustee will be unable to identify the potential risks to privacy created by the actions of its employees or its policies and procedures.

Our office finds that the RHA did not meet its duty under section 20 when it made findings inconsistent with the requirements of PHIA and placed the burden of proving a privacy breach occurred on the complainants. As a result, the RHA erred in its conclusion that the use of the PHI of the individuals was authorized.

Our office also finds that the RHA did not sufficiently investigate the privacy breach complaints and therefore was not able to identify the gaps in its process and any additional administrative safeguards as required under section 18 of PHIA.

5. The Lack of Documentation Around the Use of PHI

PHIA requires trustees to ensure that their collection, use, and disclosure of PHI is limited to the minimum amount necessary to accomplish an authorized purpose, and it is the responsibility of the trustee to ensure this standard is met. Individuals have the right to access their own PHI. This includes the right to know who has accessed their PHI and the purpose for that access.

The right of access is only meaningful when it is provided without delay in an open, accurate, and complete manner. If a trustee cannot explain to an individual who accessed their PHI or why, then the requirements under PHIA are not met.

The responsibilities of trustees to ensure the security of PHI, limit its collection, use, and disclosure and to provide meaningful access to information to individuals cannot be met if the trustee does not document who, when, what, why and how PHI is accessed by its employees. The way authorized access is demonstrated may vary between roles, but that documentation must exist.

As we have stated throughout this report, if a trustee does not meet its requirements under PHIA, does not provide meaningful access to PHI and protect the privacy rights of individuals, then the trust that citizens have in the healthcare system and its ability to protect their PHI will be negatively impacted.

Legislative Requirements

The preamble to PHIA sets out the foundation for the requirements of the act.

> *WHEREAS health information is personal and sensitive and its confidentiality must be protected so that individuals are not afraid to seek health care or to disclose sensitive information to health professionals;*
>
> *AND WHEREAS individuals need access to their own health information as a matter of fairness, to enable them to make informed decisions about health care and to request the correction of inaccurate or incomplete information about themselves; AND WHEREAS a consistent approach to personal health information is necessary because many persons other than health professionals now obtain, use and disclose personal health information in different contexts and for different purposes;*
>
> *AND WHEREAS clear and certain rules for the collection, use and disclosure of personal health information are an essential support for electronic health information systems that can improve both the quality of patient care and the management of health care resources;*

Several sections of PHIA require trustees to provide individuals access to their own PHI, and to protect the security of PHI and to limit the collection, use, and disclosure of PHI.

> ***Right to examine and copy information***
> ***5(1)*** *Subject to this Act, an individual has a right, on request, to examine and receive a copy of his or her personal health information maintained by a trustee.*
>
> ***Duty to assist an individual***
> ***6(2)*** *A trustee shall make every reasonable effort to assist an individual making a request and to respond without delay, openly, accurately and completely.*
>
> ***Restrictions on collection***
> ***13(1)*** *A trustee shall not collect personal health information about an individual unless*

(a) the information is collected for a lawful purpose connected with a function or activity of the trustee; and

(b) the collection of the information is necessary for that purpose.

Limit on amount of information collected

13(2) *A trustee shall collect only as much personal health information about an individual as is reasonably necessary to accomplish the purpose for which it is collected.*

General duty of trustees re use and disclosure

20(1) *A trustee shall not use or disclose personal health information except as authorized under this Division.*

Limit on amount of information used or disclosed

20(2) *Every use and disclosure by a trustee of personal health information must be limited to the minimum amount of information necessary to accomplish the purpose for which it is used or disclosed.*

Limit on the trustee's employees

20(3) *A trustee shall limit the use of personal health information it maintains to those of its employees and agents who need to know the information to carry out the purpose for which the information was collected or received or to carry out a purpose authorized under section 21.*

Analysis

Our office determined that most access to PHI by employees of the RHA is not documented, and there is little or no requirement for employees of the RHA to document when and why they accessed PHI. Though we recognize that there are situations that do not require the creation of separate documentation.

For example, when healthcare professionals access PHI as part of treating a patient, they typically create notes documenting their assessment and the care provided. Evidence of the purpose for this type of access is available for review and easy to explain. Creating additional documentation of the purpose for access would not be necessary.

Similarly, when employees issue bills or pharmacists fill prescriptions, these types of access generate other records that clearly show the purpose for the access and those documents are often attached or cross-referenced to the patient's medical file.

When there is a legitimate purpose for accessing PHI, there should be some documentation created that shows that purpose. Most of this documentation will be contained in the patient's file. When the purpose for the access does not allow for the documentation to be kept in the patients file, then it must still be documented and stored in a manner that enables it to be retrieved.

Situations where this is necessary could include when PHI is accessed for the purpose of research, to provide demographic information to Manitoba Health, to provide training to employees of the trustee or when the trustee is conducting an audit.

A privacy officer conducting an audit should retain copies of the audits conducted, keep a list of files reviewed, explain the purpose of the audit, and indicate what information was viewed and why it was needed to meet that purpose.

Our investigation did not find any evidence of the purpose that the facility PO accessed the PHI of one individual. Their access to this PHI was contrary to policy as they did not consult with their manager. There was no documentation on the purpose of accessing the individual's PHI, how much information was accessed or whether the RHA authorized that access.

Our office recognizes that documenting every use of PHI is difficult (or, in some cases, impossible). However, trustees must be able to indicate why information was accessed to meet their responsibilities under PHIA. Trustees should also take extra care and effort in situations where there is an increased risk of a privacy issue, such as where an employee may also be a patient of the trustee. The lack of documentation in situations where documentation should be expected is evidence that should be considered when reviewing a privacy complaint.

Documenting their collection, use, and disclosure of PHI helps trustees ensure that they are meeting their responsibilities under PHIA. Documentation also allows trustees to conduct meaningful reviews of their employees' access to PHI and identify any issues.

When trustees provide meaningful information to individuals about the access to their PHI it increases the trust in the health care system and ensures that individuals are not refusing to seek care out of fear for their privacy.

Our office also finds that the RHA did not comply with the requirements of PHIA by not documenting its access to PHI or providing sufficient information about the authorization and purpose for the access of PHI and that the minimum amount of PHI was accessed.

6. Employees ask the facility PO (and potentially others) to Access PHI for Them

One of the possible purposes the RHA gave for the facility PO accessing the PHI of the individuals was that employees would contact privacy officers and request information from patient files that they either did not have access to or did not know how to access.

Legislative Requirements

PHIA requires trustees to adopt security safeguards that protect PHI and limit the access to PHI by their employees to only the amount necessary.

> ***Duty to adopt security safeguards***
> ***18(1)*** *In accordance with any requirements of the regulations, a trustee shall protect personal health information by adopting reasonable administrative, technical and physical safeguards that ensure the confidentiality, security, accuracy and integrity of the information.*
>
> ***Specific safeguards***
> ***18(2)*** *Without limiting subsection (1), a trustee shall*
>
> *(a) implement controls that limit the persons who may use personal health information maintained by the trustee to those specifically authorized by the trustee to do so;*
>
> *(b) implement controls to ensure that personal health information maintained by the trustee cannot be used unless*

(i) the identity of the person seeking to use the information is verified as a person the trustee has authorized to use it, and

(ii) the proposed use is verified as being authorized under this Act;

(c) if the trustee uses electronic means to request disclosure of personal health information or to respond to requests for disclosure, implement procedures to prevent the interception of the information by unauthorized persons; and

(d) when responding to requests for disclosure of personal health information, ensure that the request contains sufficient detail to uniquely identify the individual the information is about.

The regulation contains the following requirements:

Access restrictions and other precautions
3 *A trustee shall*

(a) ensure that personal health information is maintained in a designated area or areas and is subject to appropriate security safeguards;

(b) limit physical access to designated areas containing personal health information to authorized persons;

(c) take reasonable precautions to protect personal health information from fire, theft, vandalism, deterioration, accidental destruction or loss and other hazards; and

(d) ensure that removable media used to record personal health information is stored securely when not in use.

Authorized access for employees and agents
5 *A trustee shall, for each of its employees and agents, determine the personal health information that he or she is authorized to access.*

Orientation and training for employees

6 *A trustee shall provide orientation and ongoing training for its employees and agents about the trustee's policy and procedures referred to in section 2.*

Information Provided by the RHA

The RHA indicated that, at times, employees at smaller clinics or with less access to PHI in the RHA's systems would contact the facility PO (who was also the Information Manager for the facility) and ask them to access patient PHI on their behalf.

Further discussion of this point revealed that, in large part, this informal practice arose from the lack of technical understanding by employees, who either did not know they could access a particular system or did not know where to find certain information in the system.

Analysis

A situation where employees ask other employees to look something up for them creates several potential issues. First, if an employee does not have access to the PHI required for the employee to complete their duties, this gap should be identified to the RHA.

This allows the RHA to ensure employees have direct access to the information they need to do their job, or provide guidance, so the employee knows where and how to find the information.

Second, if an employee does not require that information to complete their duties, then other employees, who do have access to that information, should not be providing that information to them, as this circumvents the safeguards put in place by a trustee to protect PHI.

PHIA and the regulation require trustees to limit not only what PHI the trustee collects and uses for an authorized purpose, but also what PHI each individual employee is authorized to access. Trustees are required to have processes in place to make these decisions and to update each employee's access privileges when required. For example, a nurse should have different access privileges from an administrative clerk, and their respective access privileges should be reviewed each time they change roles within the organization.

Situations where employees do not have access to the PHI, they need to complete their duties and need a colleague to access this information for them should be exceedingly rare and easily documented with the reasons for why the access is required.

A lack of employee training about how and where to access items of information in the various RHA systems resulted in employees who had an authorized purpose for accessing the information and who unknowingly also had access privileges asking a privacy officer to access that information on their behalf. This creates an issue where the privacy officer is now accessing PHI for a purpose outside of their role.

An access and privacy officer has a vastly different purpose from a nurse for accessing PHI. The RHA authorizes access based on those purposes and sets up its security safeguards and access privileges to ensure these purposes and authorizations are monitored and appropriately applied.

Access to PHI in this manner is, on the face of it, contrary to the security safeguards set up by the RHA. The purpose of those safeguards is to track who accesses PHI, when it is accessed and for what purpose.

This lack of employee training also resulted in employees asking the facility PO to access that information on their behalf. In these situations, the employee making the request may have had authorization to access the PHI, but the facility PO did not.

Additionally, because the access was done by the facility PO and was not documented, there is no way to determine whether the employee making the request was authorized to access the PHI or the purpose for the access.

PHIA requires trustees to provide their employees with ongoing training related to their policies and procedures. This should include consistent and updated training on how to use the various systems they need to complete their duties.

Without proper training in the electronic systems used by the RHA, the policies and procedures related to the security of information in those systems are of little value. If employees do not understand the systems, then they cannot properly implement the policies and procedures.

Our office finds that the RHA did not uphold its duty to adopt reasonable administrative safeguards.

In particular:

- RHA training for employees was insufficient as employees do not have the knowledge required to locate needed to locate needed information in a way that also limits their access to unnecessary information.

- RHA policies do not direct employees to raise issues related to user access privileges with their supervisors.

- The RHA does not require those with user access privileges to document when they access and share PHI for an authorized purpose with those who have less access privileges.

7. No One was Checking the Checker

The Minister of Health's guidelines for RoUAs require trustees to have a process for checking the checker. This means that the employees tasked with auditing the systems to ensure compliance are also subject to focused audit to ensure that their use of PHI is consistent with their audit function and authority.

Focused audits that check the checker can help detect and mitigate against unauthorized use. In this case, the RHA did not have established policies or procedures to track whether the actions of the facility PO were authorized. No one was checking the checker.

As mentioned in the introduction of this report, it is a significant breach of trust when the employee who is responsible for ensuring that the privacy and security of PHI is protected is also the employee who is breaching that privacy.

To maintain citizen's confidence and trust in the security of their PHI, and the healthcare system as a whole, trustees need to have consistent, robust, and reasonable measures in place to ensure that any and all employees who have access to PHI are using it in an authorized manner.

This must include measures to review any and all access of PHI by employees tasked with auditing the accesses of other employees and auditing the systems that contain PHI.

Legislative Requirements

The regulation requires trustees to create and maintain a record of user activity in accordance with guidelines set by the Minister of Health.

> ***Additional safeguards for electronic health information systems***
> ***4(1)*** *In accordance with guidelines set by the minister, a trustee shall create and maintain, or have created and maintained, a record of user activity for any electronic information system it uses to maintain personal health information.*

Section 9 of the Minister of Health's Guidelines for Records of User Activity (RoUA) sets out the requirement for trustees to "check the checker".

> ***9. Checking the Checker***
>
> *Trustees will establish a process for the occasional audit of system administrator records of activity.*

Information from the RHA

The Trustee indicated that the facility PO's responsibilities included several different kinds of audits, including both privacy-related and quality assurance audits, and responding to PHIA matters, such as complaints. The facility PO also carried out functions that were not officially part of their role, such as accessing the systems for the purpose of providing PHI to employees who did not already have access or who did not know where to find the information.

The facility and the RHA have no formal system in place for tracking any of these responsibilities. The RHA has no way of knowing when they are occurring or what files are being accessed as part of this process.

The RHA PO has started to track audits conducted by privacy officers at various hospitals and clinics within the RHA. However, the RHA has not established a process for doing so and there are no guidelines for what steps should be taken, how often such audits should occur, who is audited and who conducts the audits.

Analysis

In general, whether an access is authorized is determined largely on corroborating evidence, which works for some positions, such as employees that provide direct patient care (nurses, doctors, healthcare aides etc.) because the evidence of authorized use would be medical care records created by the health care employees that would be corroborated based upon other indicators such as employees' name, position, or shift duties.

Access to PHI by privacy officers is different. Privacy officers are responsible for ensuring that the security safeguards put in place by the RHA are sufficiently protecting PHI. Privacy officers must also enforce those safeguards by auditing the access of PHI by other employees. The evidence of the purpose for accesses of this type is the audit and if those records are not maintained, there is no way for anyone to check the checker.

The guidelines require trustees to have a process for auditing the access of PHI by employees charged with maintaining the systems and the safeguards. The RHA has no such process in place and no way to meaningfully review the accesses of PHI by privacy officers and information managers.

The facility PO had several authorized purposes for accessing PHI with no process in place to track when PHI is accessed to meet those purposes. The lack of documentation relating to these authorized purposes made checking the checker difficult if not impossible for the RHA.

Our office finds that the RHA does not have a process for checking the checker as required by the guidelines.

FINDINGS

Our office completed investigations into two complaints regarding the unauthorized access to the individuals' PHI in January of 2021 and found that a breach of privacy occurred.

Based on our office's analysis of the steps the RHA took to address the breaches and measures taken by the RHA to limit the risk of further breaches, and its compliance with PHIA, our office finds that:

1. The RHA did not meet the requirements of PHIA, the regulation, and the guidelines as it does not have a policy and process for conducting and documenting audits.

2. The RHA did not comply with its Confidentiality of Personal Health Information Policy when the facility PO accessed the individual's PHI for the purpose of an audit as the RHA's policy requires consultation with their manager and/or obtaining consent from the affected individual. Ultimately, this is a breach of the requirements under PHIA and the Regulation to ensure that PHI is used only as authorized and limited to only those who need to know the information.

3. The RHA failed to comply with PHIA and the regulations by not identifying the potential risk to the security of PHI and by not to providing sufficient training to its employees to enable them to identify that risk.

4. The RHA did not meet its duty under section 20 when it made findings inconsistent with the requirements of PHIA and placed the onus on the complainants to prove that a privacy breach occurred. As a result:

    a. The RHA erred in its conclusion that the use of the PHI of the individuals was authorized.

    b. The RHA did not sufficiently investigate the privacy breach complaints and therefore failed to identify the gaps in its process and any additional administrative safeguards that would address those gaps as required under section 18 of PHIA.

5. The RHA did not comply with the requirements of PHIA by failing to document its access to PHI and did not provide sufficient information about the authorization and purpose for the access of PHI and that the minimum amount of PHI that was accessed.

6. The RHA did not uphold its duty to adopt reasonable administrative safeguards. In particular:

a. RHA training for employees was insufficient as employees do not have the knowledge required to locate needed information in a way that also limited their access to unnecessary information.

b. The RHA policies do not direct employees to raise issues related to user access privileges with their supervisors.

c. The RHA does not require those with user access privileges to document when they access and share PHI for an authorized purpose with those who have less access privileges.

7. The RHA does not have a process for checking the checker as required by the regulation and guidelines.

UPDATE FROM THE RHA

During the course of the investigation, our office raised the issues discussed in this report with the RHA and it began working to address those issues. We also kept in contact with the RHA during the prosecution to get updates on any changes made to its policies, procedures, training, and auditing.

The RHA provided the following updates:

- The RHA will be consulting with Digital Share Services (e-Chart).

- The RHA established an Access and Privacy Interdisciplinary Team where representatives from varying programs come together to learn and share privacy matters including auditing. This team also gives those involved the opportunity to learn about the various electronic health systems being used within the RHA.

- A review of other rural health authorities auditing practices has been completed. The RHA noted that one of the health authorities has a very robust auditing program that they hope to incorporate into their own privacy program.

- The RHA provided training on auditing during its PHIA Day 2021 event.

- Quick links to account requests for access to e-Chart are available on the RHA private website. Additionally, the RHA revisited user permissions and created new ones that provide appropriate access for specific roles within the RHA.

- The RHA is developing a process for documentation in exceptional circumstances where support service employees are asked to locate PHI outside of the provision of care and are unable to record the purpose within the electronic health system.

- The RHA has quick reference guides, a learning management system and the Provincial Electronic Application Reference Library which provide staff information on the various electronic information systems and the types of PHI available in those systems.

- The RHA is developing policies that better reflect the organization's responsibilities when a conflict of interest is identified.

- The RHA's Reporting and Investigating Privacy Breaches and Complaints policy was updated and no longer directs employees to follow the "No Privacy Breach" procedure when the trustee is unable to determine whether an access was authorized.

Our office notes that much progress has been made to address several issues identified in our investigation. While the steps taken by the RHA do not fully address the issues identified by our investigation, we acknowledge that the work is ongoing.

RECOMMENDATIONS

To meet the requirements of PHIA trustees must develop a culture of privacy. Privacy must be considered and included in every aspect of the trustee's work. This can best be accomplished by ensuring it employs a privacy management program that is top-down, comprehensive, strategic, forward-thinking and embraces the privacy principles discussed throughout this report.

In light of our findings in this investigation, the Ombudsman makes six recommendations to enhance the privacy culture and program at the RHA.

To address findings number 1 and 7, the Ombudsman recommends:

> **Recommendation:** That the RHA create a policy to govern the use of audits and develop an audit program to ensure compliance with the requirements of section 18 of PHIA and section 4 of the Regulations. The audit policy and program should comply with the guidelines for auditing RoUAs.

The following recommendations are made to enhance the RHA's privacy processes, security safeguards, and employee training.

To address finding number 2, the Ombudsman recommends:

> **Recommendation:** That the RHA review and provide additional training to employees in relation to its Confidentiality of Personal Health Information Policy and its requirements in relation to conflicts of interest.

To address finding number 3, the Ombudsman recommends:

> **Recommendation:** That the RHA create a formal process and guidance for when the Trustee or its employees should consider whether there are increased risks to privacy in workplace investigations or other situations where the potential for a privacy breach exists. The guidance should address:
>
> A. potential risk factors such as the level of access to PHI and information systems, the employee's role within the Trustee, the nature of the complaint made and any other factors that may increase the risk of a privacy breach such as motive.
>
> B. what steps to take to address those risks, such as performing audits of RoUAs or changing an employee's access to information systems.
>
> C. whether to consult with, and what information should be shared with, the privacy officer.

To address finding number 4, the Ombudsman recommends:

Recommendation: That the RHA clarify in its policies, procedures, and training that where the trustee is unable to determine whether an access was authorized, the trustee should not default to considering the access to be authorized. In such situations the trustee should:

A. Review its processes to identify any gaps in its ability to determine authorization.

B. Identify any security safeguards or processes that would address those gaps and implement those safeguards and processes as soon as possible.

To address findings number 5 and 6, the Ombudsman recommends:

Recommendation: That the RHA create guidance for employees on the steps they should take if they do not have access to information or systems that they require to complete their duties. This should include a process for:

A. updating or requesting an update of user access privileges,

B. requesting access to information in emergency situations where there is no time to review and assign new user access privileges,

C. documenting accesses made in emergency situations where the person requesting access does not have user access privileges,

D. auditing emergency accesses of this type to ensure that PHI is being accessed in this way only when necessary.

Recommendation: That the RHA ensure that its employees' training includes adequate information on its electronic health information systems.

THE RHA'S RESPONSE TO THE RECOMMENDATIONS

The Ombudsman requests that the RHA respond to the recommendations in writing within 45 days of receiving this report. As this report is being sent by email to the trustee on December 31, 2024. the RHA shall respond by February 14, 2025. The RHA's response must indicate whether the RHA accepts each the recommendations. If the RHA does not accept the recommendations, then it must indicate the reasons for its refusal.

THE RHA'S COMPLIANCE WITH RECOMMENDATIONS

The Ombudsman requests that the RHA provide our office with a plan for the implementation of the recommendations within 60 days of the acceptance of the recommendations.

Jill Perron
Manitoba Ombudsman

Available in alternate formats upon request.

MANITOBA OMBUDSMAN
300 - 5 Donald Street, Winnipeg, MB R3L 2T4
204-982-9130 | 1-800-665-0531 | ombudsman@ombudsman.mb.ca
www.ombudsman.mb.ca