



**MANITOBA**  
OMBUDSMAN

Southern Health-  
Santé Sud

---

Privacy Breach:  
Use, Disclosure  
and Security of  
Information

Response to  
Recommendations Made  
in Case # MO-01541/  
2020-0251

Issue Date:  
April 2025

# THE PERSONAL HEALTH INFORMATION ACT

## RESPONSE TO INVESTIGATION REPORT RECOMMENDATIONS



# RESPONSE TO THE RECOMMENDATIONS

---

On December 31, 2024, the Ombudsman's office issued a report with recommendations following the investigation of an unauthorized use of personal health information by an employee of Southern Health-Santé Sud Regional Health Authority (the RHA). The Ombudsman's office made six recommendations:

**Recommendation 1:** 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.

**Recommendation 2:** 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.

**Recommendation 3:** 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.

**Recommendation 4:** 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.

**Recommendation 5:** 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 6:** That the RHA ensure that its employees' training includes adequate information on its electronic health information systems.

The Ombudsman requested a written response from the RHA indicating whether the recommendations were accepted by February 14, 2025. On February 10, 2025, the RHA notified our office that it fully accepted recommendations 1, 2, 3, 4, and 6. The RHA indicating that it accepted recommendation 5, with some modifications as follows:

*We acknowledge the importance of this recommendation, and while we agree with the principle behind it, we would like to recommend a modified approach.*

- A. *As noted in the investigation report, the health authority has collaborated with other health authorities within the province to create standard security roles to assign to support services staff. These security roles will be based on the permissions required for the role (i.e. junior accountants, registration clerks, health record clerks, etc.). Similar work is underway for standard security roles for clinicians, nurses and allied health professionals.*

*The processes and forms for updating user access privileges are available here. Manager's are responsible for enabling, updating and disabling user profiles. Digital Shared Services provides site management reports of inactive and active users for managers to review.*

*In light of the investigation, we recognize the need for further staff guidance and education about enabling, updating and disabling users.*

*We fully accept this recommendation.*

- B. *Providing guidance or a process for nonprivileged staff to request access to information on their behalf in emergency situations may be permissive and is incongruent with current policy, which is to never access information on behalf of another staff member.*

*Given the recent standardization of security roles and ongoing work, there should be no instances where a staff member requests access to information they are not authorized to access. We do not believe the recommendation is relevant.*

- C. *While requests for unauthorized access should not occur, there may be cases where a user with proper permissions is authorized to access a record, but the corroborating evidence difficult to verify due to time lapses between access and audit.*

*Not all electronic health systems support subsidiary notes, so reasons for access will need to be done outside of the health record.*

*We do not support requiring staff to document reasons for access, as this could create bottlenecks, privacy risks and lead to privacy paralysis. Instead, we will educate staff on the importance of corroborating evidence. If subsidiary notes cannot be made in the health record, staff will be advised to inform their manager of any potential access issues, so the manager can securely retain the details for audits and ascertain if additional training is needed.*

*We accept this recommendation with the noted modification.*

- D. *We accept this recommendation considering the modification as noted in "C".*

## CONCLUSION

---

The Ombudsman reviewed the modifications suggested by the RHA and determined that the modified recommendation adequately addressed the concerns the recommendation was based on.

The Ombudsman requested that the RHA provide a plan for the implementation of the recommendations 60 days after the recommendations were accepted. Our office received the implementation plan and will monitor the implementation of the recommendations.

April 2025  
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](mailto:ombudsman@ombudsman.mb.ca)  
[www.ombudsman.mb.ca](http://www.ombudsman.mb.ca)

