Privacy Audit Instruction Guide

Date: January 27, 2026

Shared health Soins communs Manitoba

CONTENTS

SECTION 1: INTRODUCTION

Shared Health Privacy Analyst(s) audit user activity in **key** electronic information systems managed or maintained by Digital Shared Services in accordance with the obligations set out in *The Personal Health Information Act* (PHIA). This instruction guide is intended to assist Privacy Officers and/or designates in reviewing and completing audits.

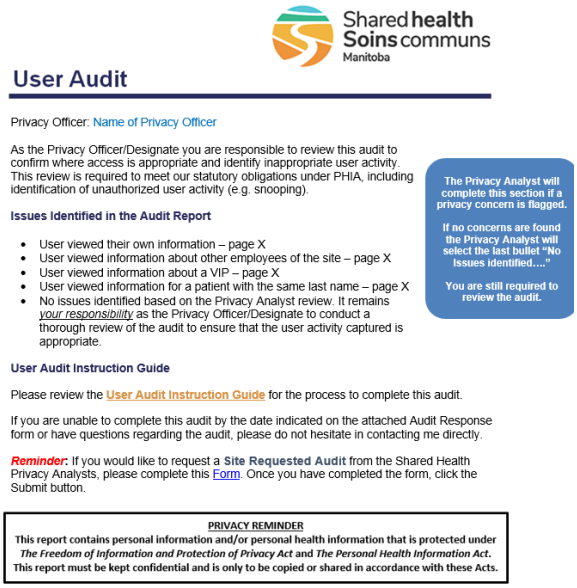
As the Site Privacy Officer and/or designate it is your responsibility to review **all** activity for the users captured on the audit and document your findings on the **Audit Response Form**. You may need to include the user's supervisor or manager to help confirm that a user's activities in a system(s) were authorized and appropriate.

SECTION 2: AUDIT PACKAGE

Figure 1 (Email Cover Page Sample)

You will receive an audit package by email that includes:

- An Email Cover Page
  - The email cover page will identify the type of audit.
- Audit Response Form
  - See Section 6.
- Password Protected Audit Report(s)



Shared health Soins communs Manitoba

User Audit

Privacy Officer: Name of Privacy Officer

As the Privacy Officer/Designate you are responsible to review this audit to confirm where access is appropriate and identify inappropriate user activity. This review is required to meet our statutory obligations under PHIA, including identification of unauthorized user activity (e.g. snooping).

Issues Identified in the Audit Report

- User viewed their own information – page X
- User viewed information about other employees of the site – page X
- User viewed information about a VIP – page X
- User viewed information for a patient with the same last name – page X
- No issues identified based on the Privacy Analyst review. It remains *your responsibility* as the Privacy Officer/Designate to conduct a thorough review of the audit to ensure that the user activity captured is appropriate.

The Privacy Analyst will complete this section if a privacy concern is flagged.

If no concerns are found the Privacy Analyst will select the last bullet "No Issues identified…."

You are still required to review the audit.

User Audit Instruction Guide

Please review the User Audit Instruction Guide for the process to complete this audit.

If you are unable to complete this audit by the date indicated on the attached Audit Response form or have questions regarding the audit, please do not hesitate in contacting me directly.

***Reminder*:** If you would like to request a **Site Requested Audit** from the Shared Health Privacy Analysts, please complete this Form. Once you have completed the form, click the Submit button.

PRIVACY REMINDER

This report contains personal information and/or personal health information that is protected under *The Freedom of Information and Protection of Privacy Act* and *The Personal Health Information Act*. This report must be kept confidential and is only to be copied or shared in accordance with these Acts.

SECTION 3: OPENING PASSWORD PROTECTED AUDIT REPORTS

Shared Health password protects all **Audit Reports.**

You will receive your password in one of two ways:

- **One time:** In a separate email from the Privacy Analyst prior to receiving an audit.
- **Annually:** This is a unique password sent to you at the start of the year. This password is to be used for all audits sent to your site until you receive a new password.

Figure 2 (Password email Sample)

Shared health Soins communs Manitoba

Additional Audit Information for 2025

Privacy Officers: XXXXXXX

As of January 1, 2025, this will be your new password for all audits sent to you:

???audit2025!

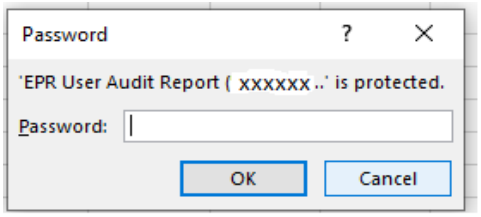
Please retain this email and remember your password. It is effective until December 31, 2025. You can share this password with other staff within your facility/region who will assit you in conducting Shared Health audits.

If you have any questions about the audit or are no longer the Site Privacy Officer/Designate at your site, please contact privacy@sharedhealthmb.ca

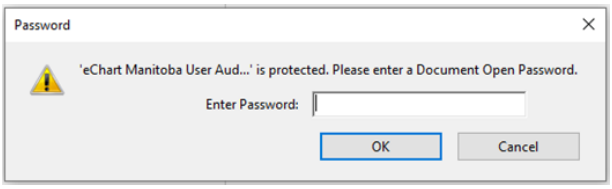
Reminder: If you would like to request a **Site Requested Audit** from the Shared Health Privacy Analysts, please complete this **Form**. Once you have completed the form, click the Submit button.

When you receive the email, open the attached **Audit Report**, enter the password and click OK. The **Audit Report** will open for your review.

Figure 3 (Password Prompt Sample)



OR



SECTION 4: FLAGGING QUESTIONABLE ACTIVITY

The Privacy Analyst conducts a comprehensive review of all audits based on information provided and/or available.

The Shared Health Privacy Analyst will “flag” any questionable activity identified during their review.

- These issues are listed within the “**Issues Identified in the Audit Report**” section of the email cover page as shown in Figure 1.
- It is the Site Privacy Officer and/or designate’s responsibility to conduct a full review of the **Audit Report** and to confirm the identified issues using the **Audit Response Form**.

SECTION 5: REVIEWING THE AUDIT REPORT

As the Site Privacy Officer and/or designate, you are required to conduct a thorough review of the **Audit Report** to determine if the users audited have appropriately accessed the information in the electronic information system(s). Section 6 provides a list of things you should consider as part of your review.

Additional Support

- **Supervisor, Manager, Program Director**

  There are times when you may need to include the user's supervisor, manager or program director to confirm whether the access was appropriate. You are required to include their responses on the **Audit Response Form**.

- **Privacy Analyst**

  You can contact the Privacy Analyst who ran the audit if you have questions regarding the audit, what to do if you identify a breach or if something doesn't look right.

  If you forward the **Audit Response Form** and **Audit Report** for review, you must collect responses from the reviewer, review the audit yourself and return the completed **Audit Response Form** to:

  - Email: privacy@sharedhealthmb.ca
  - Fax: 204-926-9148 (in Winnipeg)

Note: When forwarding the **Audit Report** to someone else you must maintain the appropriate safeguards to protect the personal health information contained in the reports. Always password protect the documents.

SECTION 6: THINGS TO CONSIDER DURING YOUR AUDIT REVIEW

The following are considerations as you review the **Audit Report(s)**:

- Did the user view information about an individual who is not a patient at the site?
- Did the user view information about other employees?
- Did the user view information about VIPS (e.g. celebrities, politicians or other high visibility community individuals)?
- Did the user view their own personal health information?
- Did the user view information about a patient who has the same last name?
- Did the user view information outside working hours based on the dates and times of access?

These accesses may require further review!

For assistance contact the Privacy Analyst who provided the audit.

- Did the user have a high volume of access to a specific record about an individual over a short period of time or a consistent pattern over time?
- Did the user (e.g. an Account Clerk) access certain types of information outside the person's role (e.g., a patient's visit history, lab results, most recent room assignment, etc.)?

SECTION 7: SITE REQUESTED AUDIT OR ADDITIONAL AUDIT INFORMATION

If additional information is required to facilitate your review, you can request additional audit(s) using this **Site Requested Audit Form**.

This form can also be used to request a new (separate) audit if you have specific concerns, such as (but not limited to):

- Suspected non-compliance with policies or procedures;
- Management audit requests;
- Patient concerns or complaints;
- Staff reported issues or observations;
- Follow-up on previous audit findings;
- Pro-active audit on staff at your site at any time.

SECTION 8: COMPLETING THE AUDIT RESPONSE FORM

When possible, complete the **Audit Response Form** electronically. The **Audit Response Form** must be completed in its entirety for all identified users with or without flagged activity.

Figure 4 (Audit Response Form)

Section 36 of The Freedom of Information and Protection of Privacy Act (FIPPA) permits Shared Health to collect information about user activity.

Audit Response Form

Privacy Audit Number:	N/A
Privacy Officer/designate:	Name of Privacy Officer(s) assigned at you site
Authorized Sponsor:	Name of Authorized Sponsor assigned at your site
Site:	Name of site being audited
Date Audit Issued:	February 6, 2026 (Date when audit is sent)
Reason for Audit:	**Site Requested Audit** (as an example)
System Audited:	**eChart and EPR** (As an example)
Active User(s) Audited:	**(4)** ***Only user(s) with activity (active users) are listed below.***
Inactive User(s) Audited:	**(2)**
Total Users Audited:	**(6)**
Date Range:	**From** January 1, 2026 **To** January 31, 2026

Completed form due by: **February 27, 2026**

The User Audit Report contains information about user activity. Once you have completed your review of the report, document your findings below **for your site.** The Shared Health Privacy Office is authorized to collect this information under section 36 of FIPPA.

c. ***Total number of individual breaches identified on this audit (select a number):*** Choose number.

User's Name	a. Appropriate Access Confirmed At Your Site	b. Comments (Include additional information whenever possible)
Test Patient #1	☐ Yes ☐ No	Choose an item.
Test Patient #2	☐ Yes ☐ No	Choose an item.
Test Patient #3	☐ Yes ☐ No	Choose an item.
Test Patient #4	☐ Yes ☐ No	Choose an item.

d. **Privacy Officer name:**	e. **Date:** Click here to enter a date.
Click here to enter text.	

For assistance or additional information, contact
Name Of Privacy Analyst, Privacy Analyst, Phone Number or email address

Please submit the completed form to:
privacy@sharedhealthmb.ca
Fax: 204-926-9148 (in Winnipeg)

For helpful tips on how to complete a User Audit, refer to the User Audit Instruction Guide:
User Audit Instruction Guide

a) In the column, **Appropriate Access Confirmed At Your Site**, check Yes or No.

b) In the column, **Comments** you can select from the drop-down menu of responses:

- Appropriate access.
- Confirmed Breach-Audit closed.
- Investigation underway: (type here to include additional information).
- User works at multiple sites. User had appropriate access at this site. Unable to confirm the following access: (type here to include dates you were unable to confirm).

- No user activity during audit date range at this site. (type here to include additional information).
- User no longer works at site: (type here to include additional information).
- Other: (type here to include additional information).

c) Select the **"Total number of individual breaches identified on this audit"** from the drop down

- If no inappropriate access was found during the audit review, the number to select is 0 (none), or
- Count each specific user with a breach as a separate instance. The total count reflects the number of breaches themselves, not just the number of people in violation.

    - Example 1: If an audit identified three separate instances of a single user snooping, the reported number is 3.

    - Example 2: If two distinct individuals committed breaches, but one individual had two separate, reportable breaches while the other had one, the total number to report is 3.

d) Sign the form by typing your name directly.

e) Select the completion date using the drop-down calendar.

Figure 4 (Completed Audit Response Form)

Audit Response Form

Privacy Audit Number:	N/A
Privacy Officer/designate:	Name of Privacy Officer(s) assigned at you site
Authorized Sponsor:	Name of Authorized Sponsor assigned at your site
Site:	Name of site being audited
Date Audit Issued:	February 6, 2026 (Date when audit is sent)
Reason for Audit:	**Site Requested Audit** (as an example)
System Audited:	**eChart and EPR** (As an example)
Active User(s) Audited:	**(4)** ***Only user(s) with activity (active users) are listed below.***
Inactive User(s) Audited:	**(2)**
Total Users Audited:	**(6)**
Date Range:	**From** January 1, 2026 **To** January 31, 2026

Completed form due by: **February 27, 2026**

The User Audit Report contains information about user activity. Once you have completed your review of the report, document your findings below **for your site.** The Shared Health Privacy Office is authorized to collect this information under section 36 of FIPPA.

c. ***Total number of individual breaches identified on this audit (select a number):*** Choose number.

User's Name	a. Appropriate Access Confirmed At Your Site	b. Comments (Include additional information whenever possible)
Test Patient #1	☐ Yes ☐ No	Appropriate access.
Test Patient #2	☐ Yes ☐ No	User works at multiple sites. User had appropriate access at this site. Unable to confirm the following access: January 5-10 and January 18, 21 and 25.
Test Patient #3	☐ Yes ☐ No	Appropriate access.
Test Patient #4	☐ Yes ☐ No	User no longer works at site: Manager will submit paperwork to disable user's access. User also works at clinic XXX.

d. **Privacy Officer name:**	e. **Date:** Click here to enter a date.
Click here to enter text.	

For assistance or additional information, contact
Name Of Privacy Analyst, Privacy Analyst, Phone Number or email address

Please submit the completed form to:
privacy@sharedhealthmb.ca
Fax: 204-926-9148 (in Winnipeg)

For helpful tips on how to complete a User Audit, refer to the User Audit Instruction Guide:
User Audit Instruction Guide

SECTION 9: RETURN THE AUDIT RESPONSE FORM

Once you have completed your review of the **Audit Report**, return it by:

- **Email:** To the shared mailbox privacy@sharedhealthmb.ca, or
- **Fax:** You can send the form to 204-926-9148 (in Winnipeg).

If you are unable to complete the audit by the due date, need assistance or additional information, contact the Shared Health Privacy Analyst who sent you the audit.

Do not return the **Audit Report(s)**.

SECTION 10: PRIVACY SAFEGUARDS

The **Audit Report** contains personal health information. You must ensure that appropriate safeguards are always in place to protect the confidentiality of this information:

- Do not forward this email or the report to anyone outside your organization.
- Only share the **Audit Report** and password with persons required to participate in the audit review.
- Contact the Shared Health Privacy Analyst if you have any questions about sharing the **Audit Report**.

SECTION 11: ADDITIONAL INFORMATION RELATED TO ECHART AUDITS

For additional information on the eChart audit process, refer to:

Handbook for Site Privacy Officers (refer to Section 5):
https://echartmanitoba.ca/files/echart-mb-handbook-site-privacy-officers.pdf

If a user viewed their own personal health information (PHI) or the PHI of another individual that is not in support of patient care, the following can be used:

Inappropriate Access by eChart User Information sheet
https://home.sharedhealthmb.ca/wp-content/uploads/echart-inappropriate-user-access-info-sheet.pdf

For a change of eChart Manitoba Site Contact Information, such as Privacy Designate, Authorized Sponsor, Authorized Account Requestor, IT Resource, All Roles Assigned Currently and Outage Contact complete the:

eChart Manitoba Site Contact Update Form
https://echartmanitoba.ca/files/echart-site-contacts-update-form.pdf

SECTION 12: REQUEST TO REMOVE/ADD/DISABLE/LEAVE OF ABSENCE USER ACCESS

Use the **eChart Account and Access Request Form** to request the removal of user access (e.g. for a user identified in an audit who no longer works at your site), or the **Site Contacts Update Form** to request any changes to site contacts (e.g. a new privacy officer or designate).

For more information, visit: https://echartmanitoba.ca/hcp/forms/

For all **other electronic information systems** managed or maintained by Digital Shared Services send an email to the Service Desk at servicedesk@sharedhealthmb.ca or call 204-940-8500. If you have access to Ivanti Service Manager (ITSM) you can go to the Service Catalog and select “Provincial Request for Access” and make the necessary requested changes.