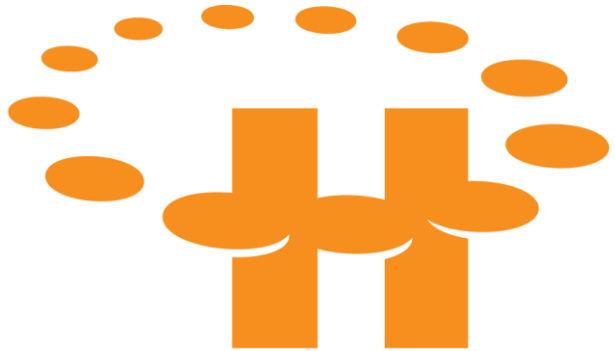
2017

Telus PS Suite Privacy Audit Guide



Hamilton Family Health Team

Better care, together.

Anson Trinh, Vanessa Foreman, and Sari Ackerman

Hamilton Family Health Team

4/19/2017

Introduction

There is no doubt that concerns about privacy are growing, including in the health care sector. In June 2016, Ontario's new privacy legislation was enacted with the aim of better protecting patient privacy and improving transparency in the health care system. More changes are expected once the Bill's regulations come into effect.

Within the HFHT, each family physician is a Health Information Custodian (HIC). HICs are responsible for taking reasonable steps to ensure that the collection, use and disclosure of patients' personal health information is for authorized purposes only. Unauthorized "use" now explicitly includes the unauthorized viewing of personal health information in EMRs, regardless of the motive, e.g., curiosity, personal gain, concern about the health and well-being of individuals, interpersonal conflicts, etc.

One way to help identify whether there has been unauthorized access to patients' personal health information (e.g., "snooping") is to conduct an EMR audit. This EMR Audit Reports Guide provides instructions for running various types of audits on the Telus PS EMR, and some information about how to interpret the results of each audit type. The audit reports will only provide information about user activity in the EMR. You may need to collect additional information if the audit suggests that inappropriate or unauthorized access to patients' personal health information (i.e., a "privacy breach") may have taken place. The steps on page 10 of this guide can offer some general guidance on next steps.

How to Use This Guide

There are several types of audits that you can run in the Telus PS EMR; however, there are only two types of audits that record every transaction or change done in the patient chart. These logs can be viewed by specific patient or by specific user account:

Who	Report Type	Page No.
Specific patient or specific user activity	Transaction Logs	3

It is recommended that a process for conducting regular audits be established. Auditing specific patients who are more likely to be targets of snooping should be done at least once annually; however, more frequent audits will decrease the amount of records to review and may help make audits more manageable and meaningful.

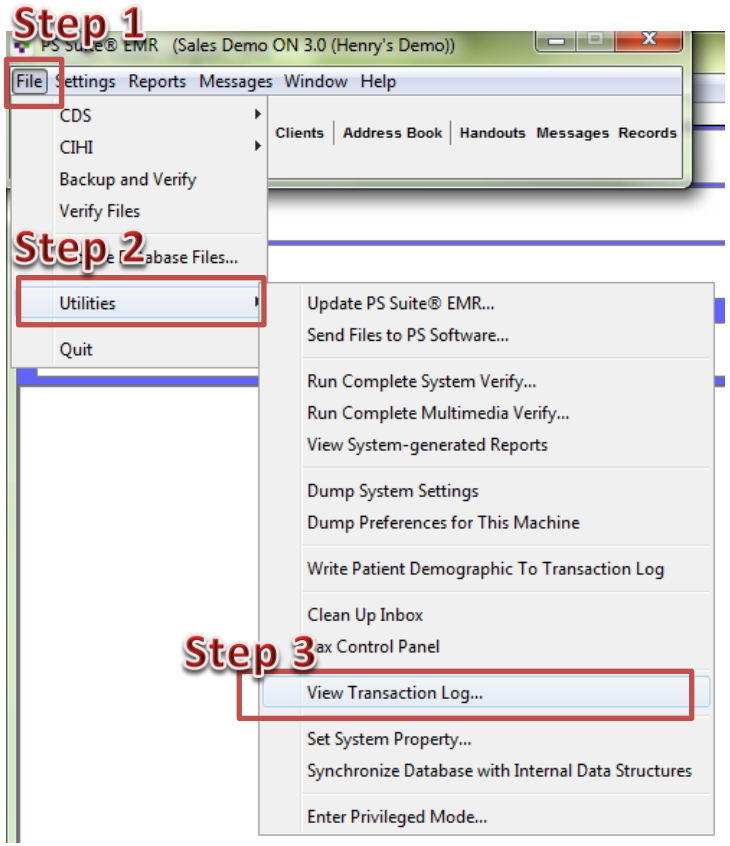
Other audit types might be more suitable if you are conducting a more general and broader review of user activity in your EMR:

Transaction Logs

Description: Every change that users make in PS Suite EMR is recorded in a transaction log. The log records everything that is done in a patient's chart, such as viewing a patient record, entering notes, editing or deleting any information, and sending messages. The log also records some non-clinical changes, such as appointments that were booked and changes to health card numbers. Billing data is not recorded in the transaction log. The log includes which user did the work, when, and from which workstation. The transaction log is your medico-legal audit trail.

At the time of writing this guide, the log currently does not capture the duration of time that a user has a chart opened.

Use: Administrators may choose to run this report for random chart audits, to investigate specific records, or to investigate activity by user to review for unauthorized access. There are many different types of transactions that are available in the logs. Each of them are described within the Administrator Guide v5.3 available from Telus.

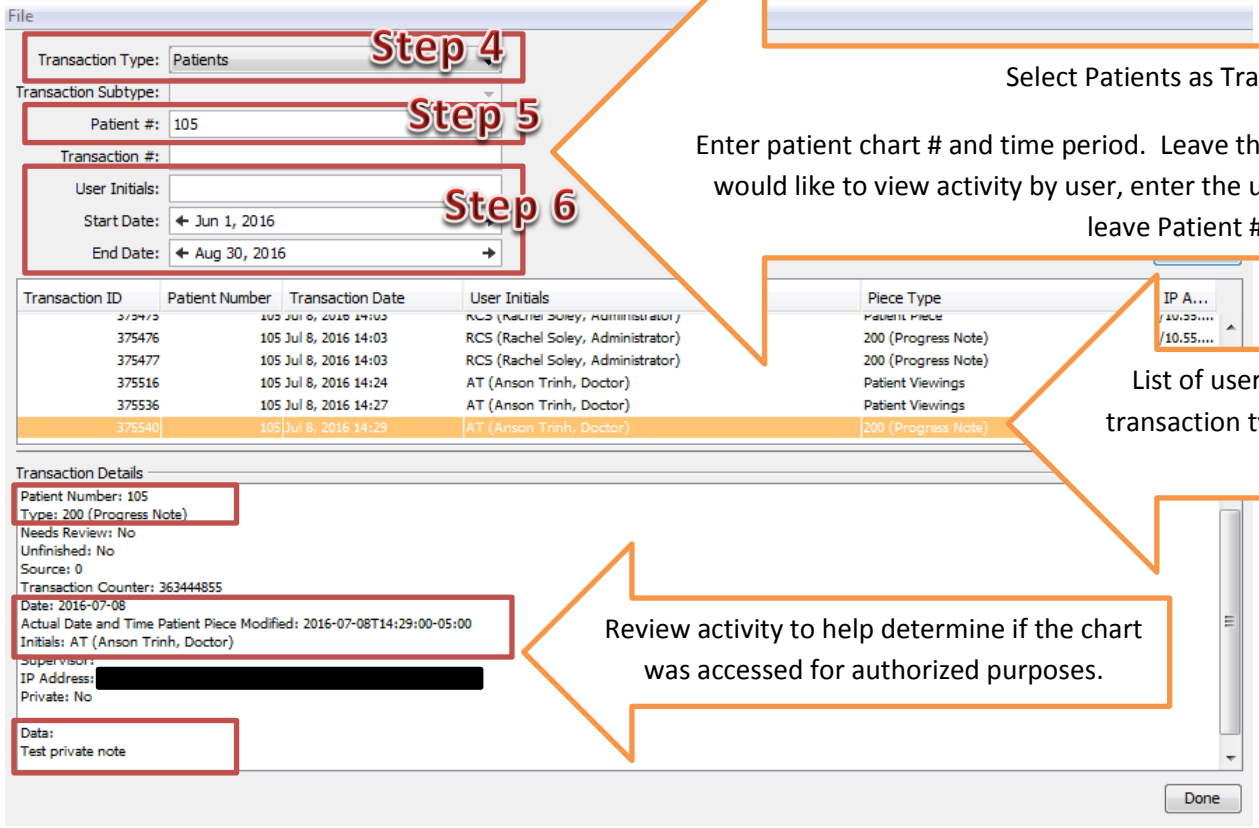


Instructions:

From the main toolbar, click **File**, then **Utilities** and then **View Transaction Log**. Depending on your version of the EMR you may be prompted to enter a permission code which can be obtained by contacting Telus PS Suite Support.

It is recommended to select **Patients** as the Transaction Type.

The **Patients** transaction type will include all activities including viewings and data modification or entry. As this report will reveal personal health information, the system will display this warning and prompt for a user password. This log can be helpful in determining reasons for accessing a chart. For instance, a Patient Viewing transaction followed up by either a Demographic or Progress Note transaction within a few minutes usually indicates that the user had a reason to access the chart related to patient care.



Select Patients as Transaction Type

Enter patient chart # and time period. Leave the User Initials field blank. If instead you would like to view activity by user, enter the user initials in the User Initials field and leave Patient # blank.

List of users who have accessed the chart and the transaction type. Click on a row for additional details.

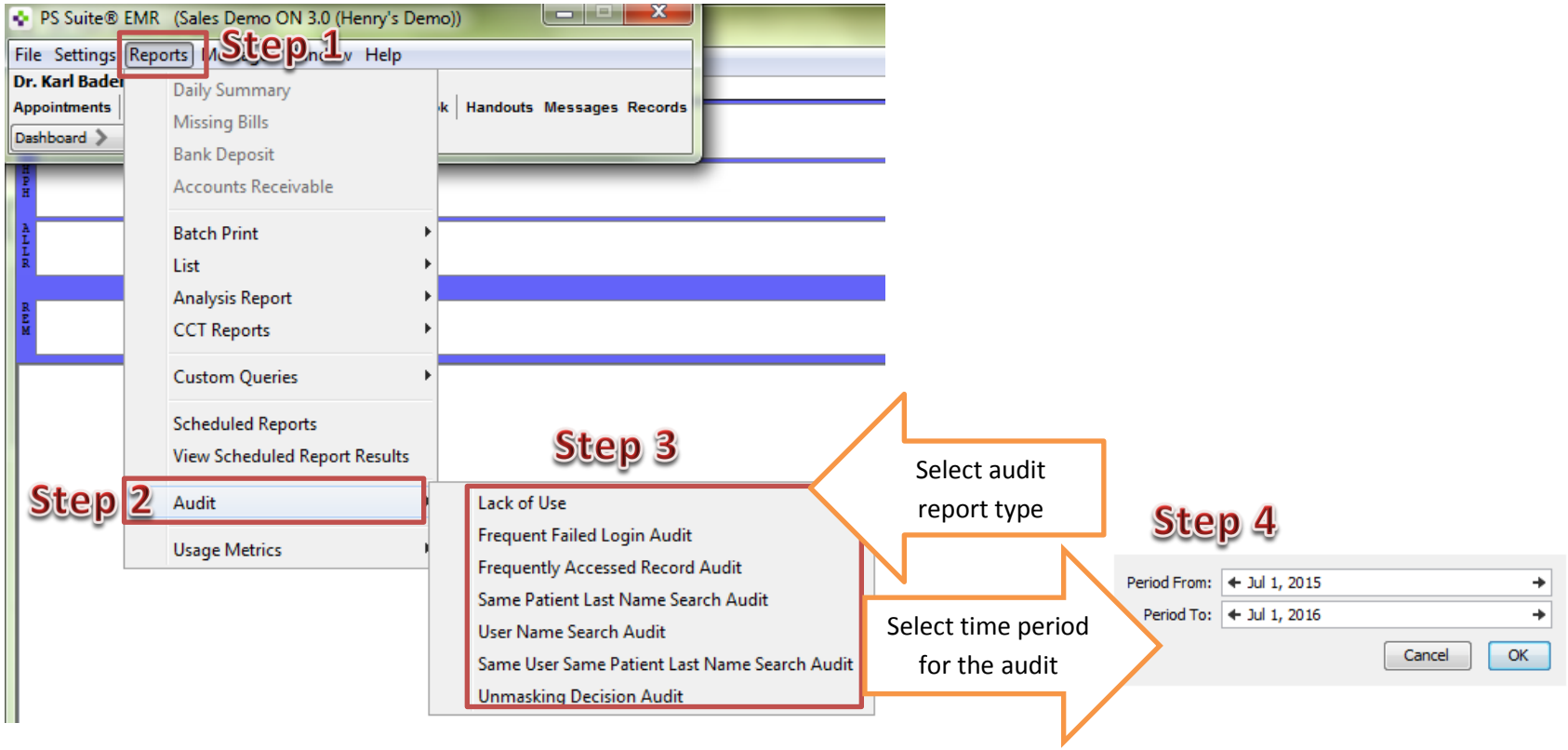
Review activity to help determine if the chart was accessed for authorized purposes.

Audit Reports

The Telus PS Suite EMR has standard general audit reports that users can utilize as part of their privacy audit activities. The most relevant reports are described below along with a guideline on how to use them.

Instructions:

Reports can be accessed from the main toolbar. Click on **Reports** and then choose **Audit**. Then, select the type of audit report and time period:

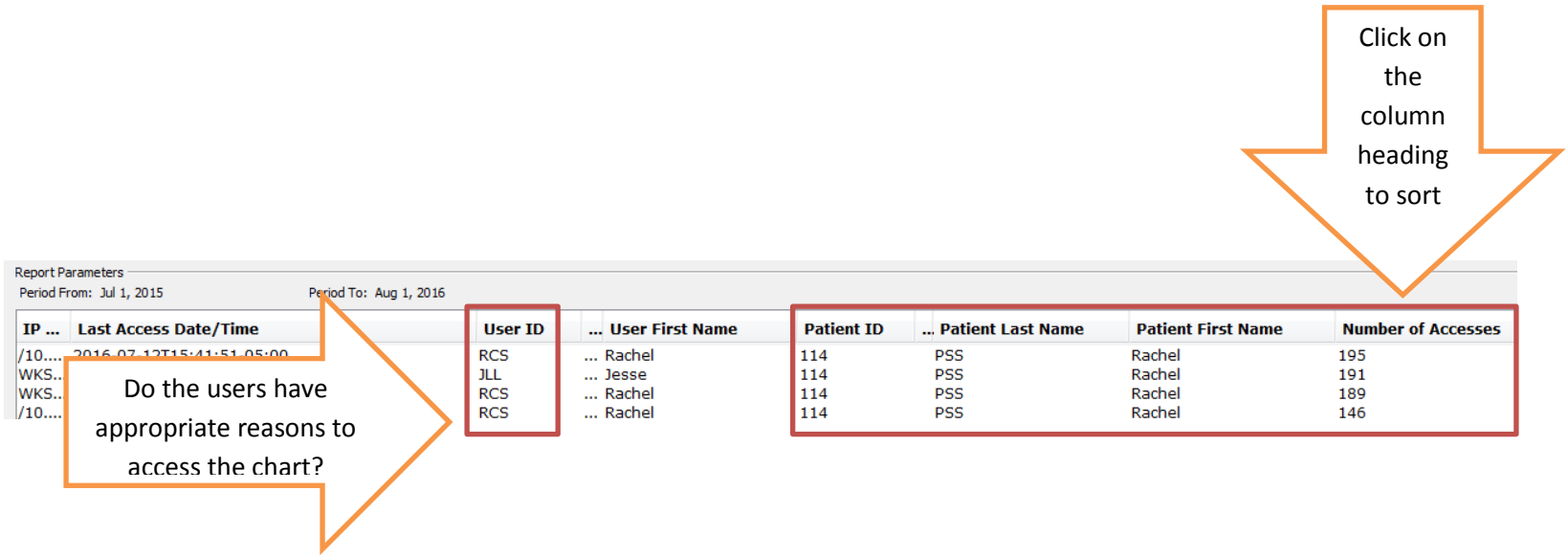


A) Frequently Accessed Records Audit

Description: This report lists patient records that have been accessed a high number of times in a specified time period or records that have been accessed by a large number of different users.

Use:

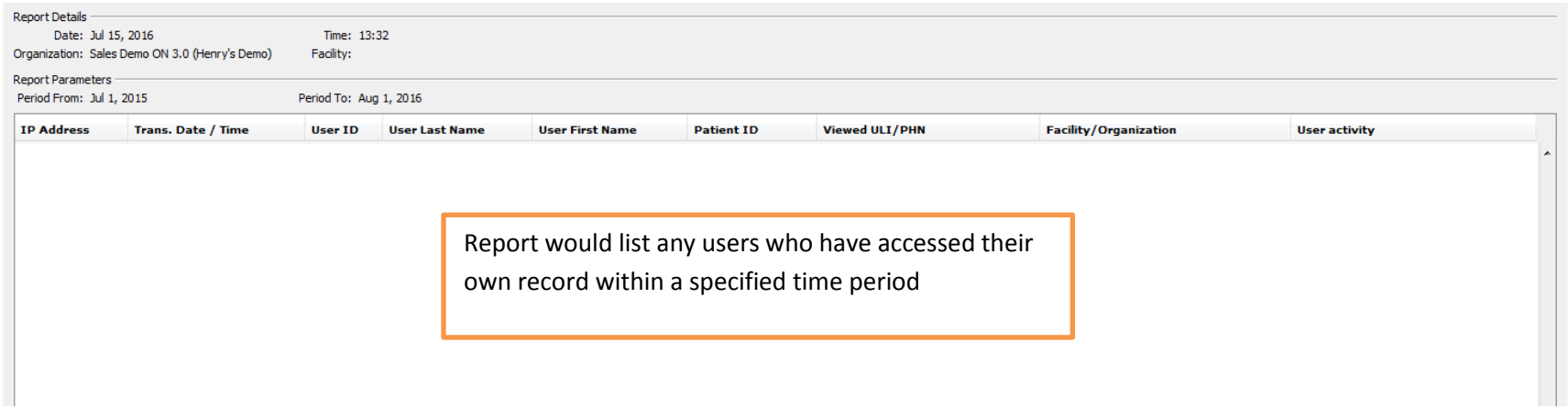
Look for records that have been accessed an abnormally high number of times and try to determine if the users who have accessed the records are those that are part of providing the patient care or support. If it cannot be determined that the user had appropriate reasons for accessing the record that number of times, this should be investigated further.



B) User Name Search Audit

Description: Generates a list of users who accessed their own personal record within a specified period.

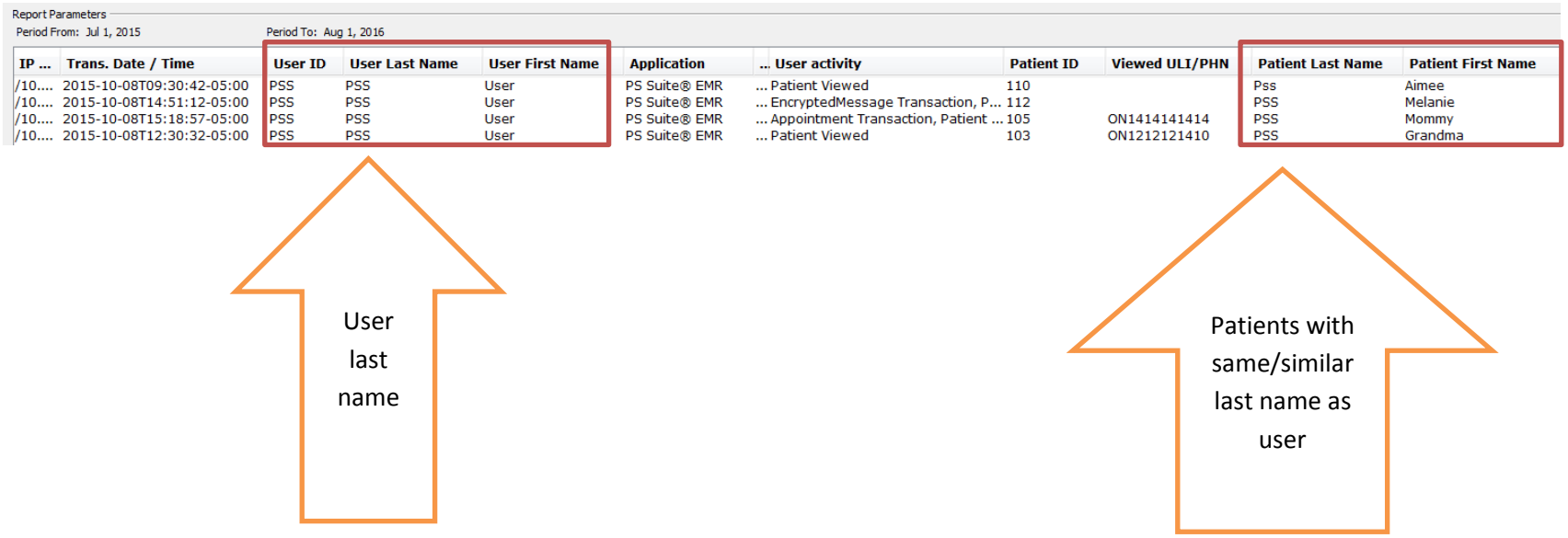
Use: Users who wish to access their own personal health records should only do so by following the relevant organizational privacy policies and procedures.



C) Same User Same Patient Last Name Search Audit

Description: Generates a list of users who accessed the records of patients who have similar last names as them within a specified period. For example, the user John Johnson accessed records for patients Bob Johnson, Jane Johnson, and Mary Jonson.

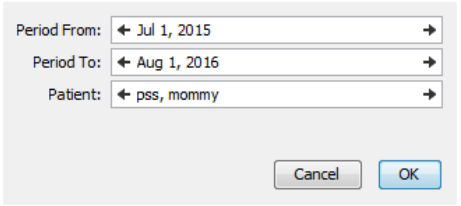
Use: Some patients may have family relationships with employees of the office; however, just because a person is related to the patient does not mean that they have free access to the family member's health record. For some common last names, it might be normal for someone who is treating an unrelated patient with the same last name.



D) Unmasking Decision Audit

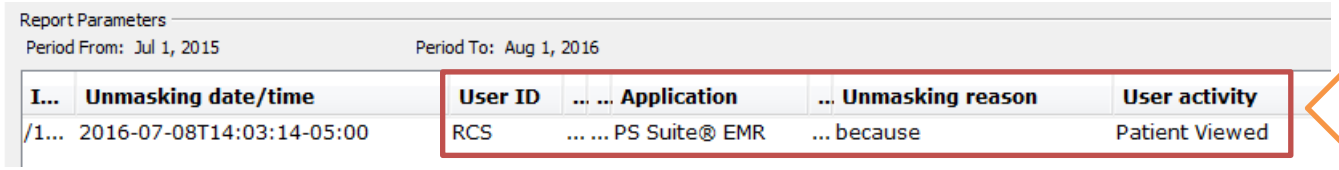
Description: Generates a list of users who broke a patient "lockbox" and accessed a specific patient's record (full patient chart or specific private notes) within a specified period.

Use: Enter in the patient name or ID of records who are known to have their record or parts of their record marked as private. Users who try to access a locked chart will be prompted by the system that the record is private and may only be accessed in the case of an emergency. Users who wish to continue to try to access the record will be requested to enter the cause for accessing. If any users are found to have "broken the lockbox", determine if they had reasonable cause to have accessed the record.



Patient known to have the chart or parts of the chart marked as private

Enter patient name or chart #



Users who have "broken the lockbox" to view the private chart

If you observe suspicious activity in your EMR

After you interpret the results of the audit reports, you may conclude that there is suspicious user activity in your EMR. Below are steps to take to address this issue:

1. Ensure that you have interpreted the audit reports accurately. If concern about user activity remains, investigate further by meeting with the user to verify his or her activities in the record.
2. If it has been determined that access did not fall under authorized collection, use or disclosure according to relevant privacy legislation, then a privacy breach has been committed.
3. The Hamilton Family Health Team's Privacy Breach Protocol (included as an Appendix) provides step-by-step instructions about what to do next.

If you need help

If you have questions about an actual or suspected privacy breach, please contact:

Dr. Lindsey George, HFHT Privacy Officer
Lindsey.George@hamiltonfht.ca (please do not use identifying information in your email)
905-667-4848 ext. 117

If you are unable to reach Lindsey, you may also contact:

Vanessa Foreman, Health Planning & Communications Coordinator (and support to Dr. George with respect to HFHT Privacy Policies)
Vanessa.Foreman@hamiltonfht.ca (please do not use identifying information in your email)
905-667-4848 ext. 128

If you have questions related to performing audits in Telus PS, please contact your Quality Improvement Decision Support Specialist (QIDSS).

Appendix 1.1

Hamilton Family Health Team

Privacy Breach Protocol[1]

Report

If a privacy breach happens within an individual family physician's office and it can be addressed there, then it should be and also should be reported to the relevant FHO's lead physician. If a privacy breach cannot be managed within the family physician's office, the Privacy Officers can be contacted to assist.

Annually each FHO will submit a report to the Privacy Officers who will make a full report to the board of the Hamilton Family Health Team.

Privacy Breach

A privacy breach happens whenever a person contravenes or is about to contravene a rule under the *Personal Health Information Protection Act, 2004* (PHIPA) or our privacy policies. The most obvious privacy breaches happen when patient information is lost, stolen or accessed by someone without authorization.

For example:

- A fax is misdirected
- An unencrypted laptop with health information saved on the hard drive is stolen
- A courier package is not delivered to the correct address
- A USB key is lost
- A patient reads another patient's health record on a computer while waiting in a clinic room
- A test result is filed in the wrong health record
- Someone talks about a patient of the Family Health Team with a friend
- Health records to be disposed of are recycled and not shredded
- Out of curiosity, a staff member reviews a neighbour's health record

[1] Based on the Information and Privacy Commissioner/Ontario "What to Do When Faced with a Privacy Breach? Guidelines for the Health Sector". Available online: http://www.ipc.on.ca/images/Resources/up-hprivbreach.pdf

- Health information is given to the media
- A staff member makes a copy of an ex-spouse's health record without the permission of the patient

Privacy Breach Protocol

The following steps will be taken by the Privacy Officers (or delegate) if they believe there has been a privacy breach:

Step 1: Respond immediately by implementing the privacy breach protocol

- Ensure appropriate staff members within the Hamilton Family Health Team and the applicable Family Health Organization are immediately notified of the breach, including the Privacy Officers and the physicians whose patients are potentially affected by the privacy breach.

- Address the priorities of containment and notification as set out in the following steps.

Step 2: Containment - Identify the scope of the potential breach and take steps to contain it

- Retrieve the hard copies of any personal health information that has been disclosed.

- Ensure that no copies of personal health information have been made or retained by the individual who was not authorized to receive the information and obtain the person's contact information in the event that follow-up is required.

- Determine whether the privacy breach would allow unauthorized access to any other personal health information (e.g. an electronic information system) and take whatever necessary steps are appropriate (e.g. change passwords, identification numbers and/or temporarily shut down a system).

- Consider notifying the Information and Privacy Commissioner/Ontario (IPC/O) and/or legal counsel if appropriate.

Step 3: Notification - Identify those individuals whose privacy was breached and notify them of the breach

- At the first reasonable opportunity, any affected patients (or others whose personal health information has been affected) will be notified.

- The type of notification will be determined based on the circumstances (such as the sensitivity of the personal health information, the number of people affected, and the potential effect the notification will have on the patient(s)).

    - For example, notification may be by telephone or in writing, or depending on the circumstances, a notation made in the patient's file to be discussed at his/her next appointment.

- Provide details of the extent of the breach and the specifics of the personal health information at issue.
- Advise affected patients of the steps that have been or will be taken to address the breach, both immediate and long-term.
- Consider notifying the IPC/O and/or legal counsel if appropriate.

Step 4: Investigation and Remediation

- Conduct an internal investigation into the matter. The objectives of the investigation will be to:
    - Ensure the immediate requirements of containment and notification have been addressed.
    - Review the circumstances surrounding the breach.
    - Review the adequacy of existing policies and procedures in protecting personal health information.
    - Address the situation on a systemic basis.
    - Identify opportunities to prevent a similar breach from happening in the future.
- Change practices as necessary.
- Ensure staff are appropriately re-educated and re-trained with respect to compliance with the privacy protection provisions of PHIPA and the circumstances of the breach and the recommendations of how to avoid it in the future.
- Continue notification obligations to affected individuals as appropriate.
- Consider notifying the IPC/O and/or legal counsel as appropriate.
- Consider any disciplinary consequences with staff or contract issues with independent contractors or vendors that follow from the privacy breach.

Appendix 1.2 Audit Tracking Worksheet

Date:	Audit Conducted by:	Type of Audit:	Abnormal Findings? (Yes/No)	Comments: