2017

P&P Privacy Audit Guide

Anson Trinh, Vanessa Foreman, Sari Ackerman, and Joshua Tseng
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 P&P 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 13 of this guide can offer some general guidance on next steps.

How to Use This Guide

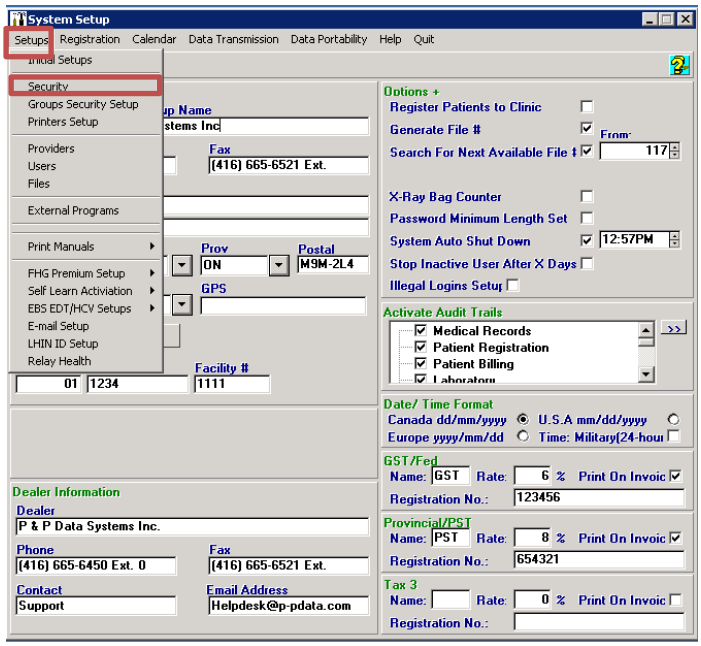
If this is the first time that privacy audits are being conducted, you may need to setup access to the modules. In some cases, only certain users will have access to the audit setup so you may need to check within your office to determine which user has the correct privileges.

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.

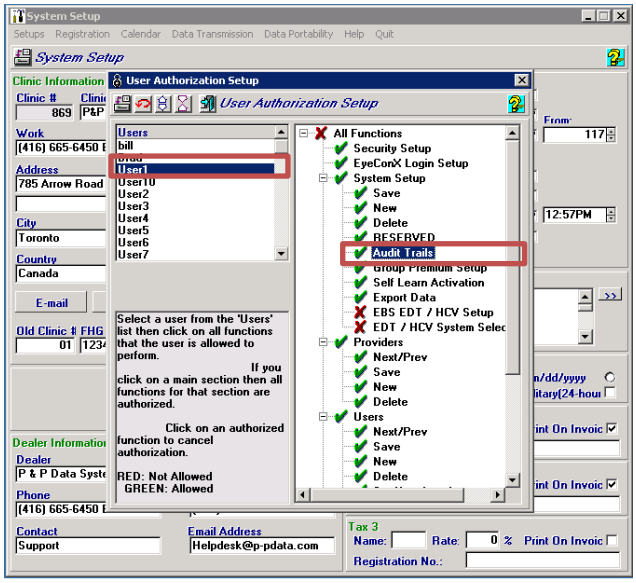
Accessing the Audit Trails

1. Log onto P&P and click on **Utilities**.

2. On the top toolbar, click **Setups**, then **Security**.

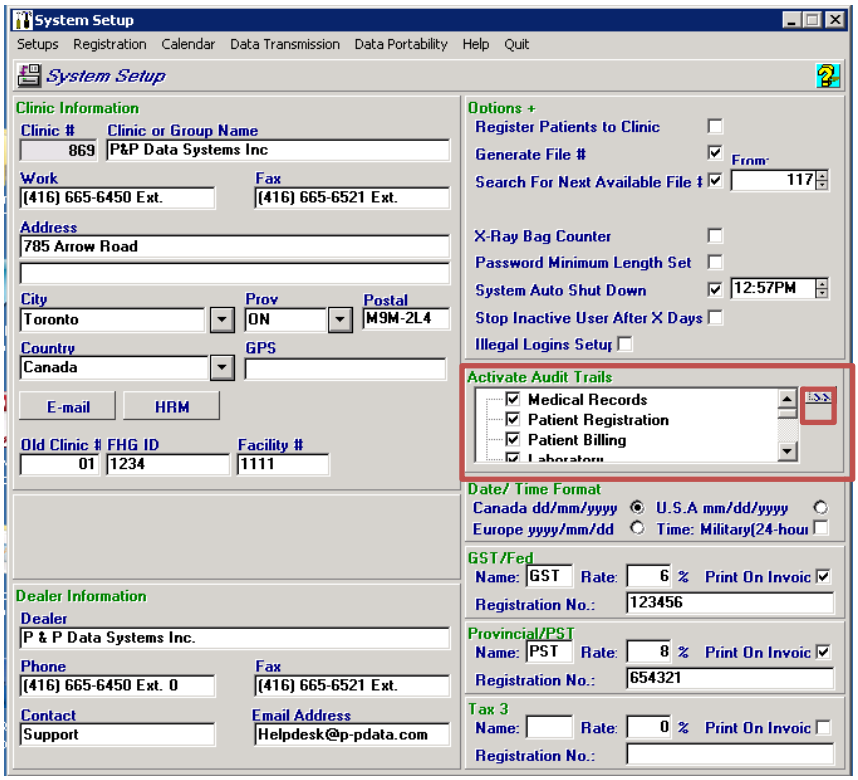


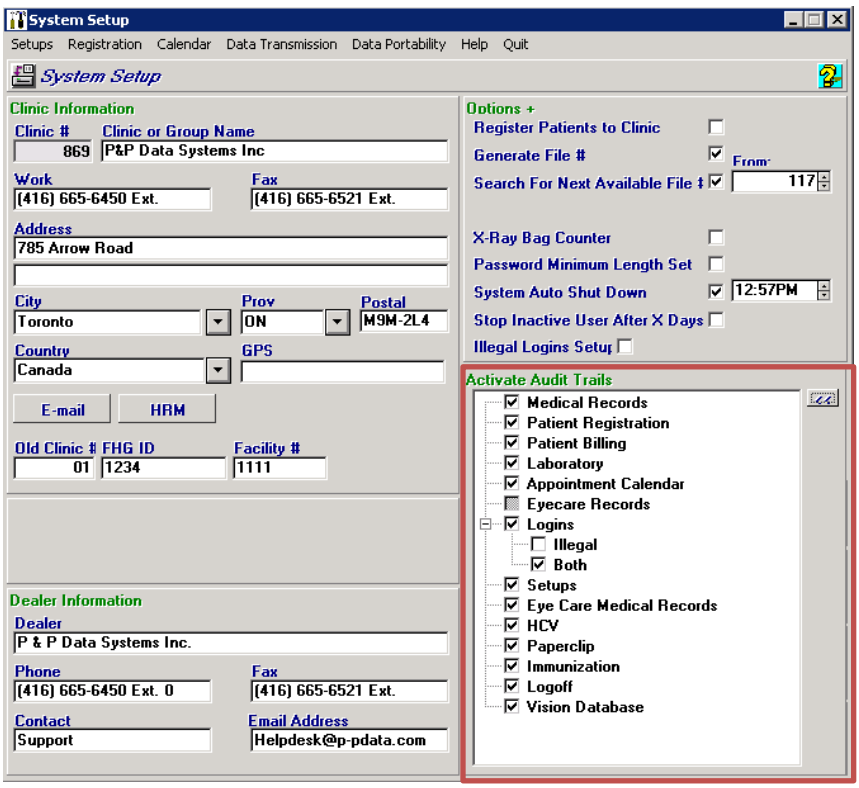
3. The User Authorization Setup window will appear. Select the user you wish to grant access to the audit trails (you can select yourself). Then, under the System Setup category, make sure the **Audit Trails option** has a green checkmark. If it is a red X, click on the red X to make it a green checkmark. (Likewise, you can deny access by making the green checkmark into the red X by clicking on it again).



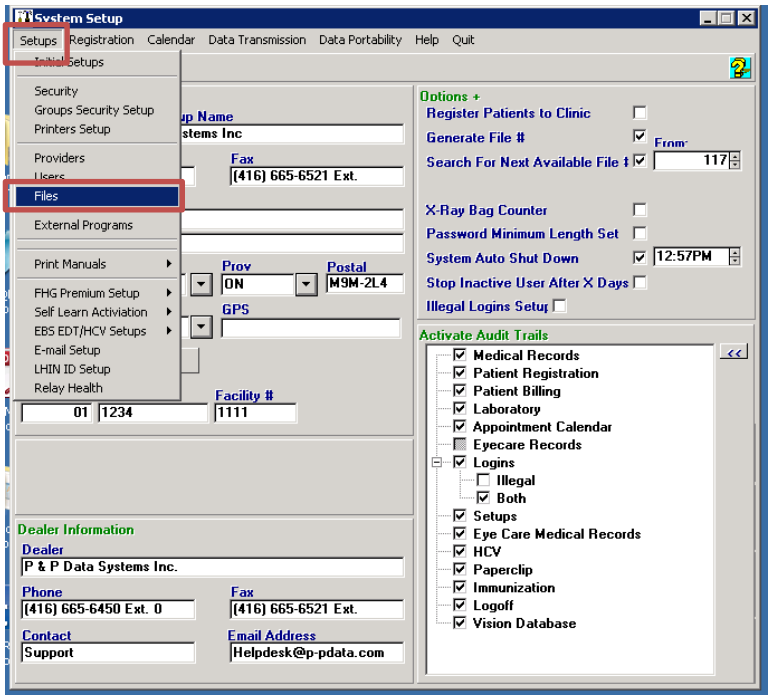
4. Click ( ) to save and ( ) to exit.

5. Under the *Activate Audit Trails* section, select the modules you wish to have audited. Click the double arrow to expand and see all the modules.

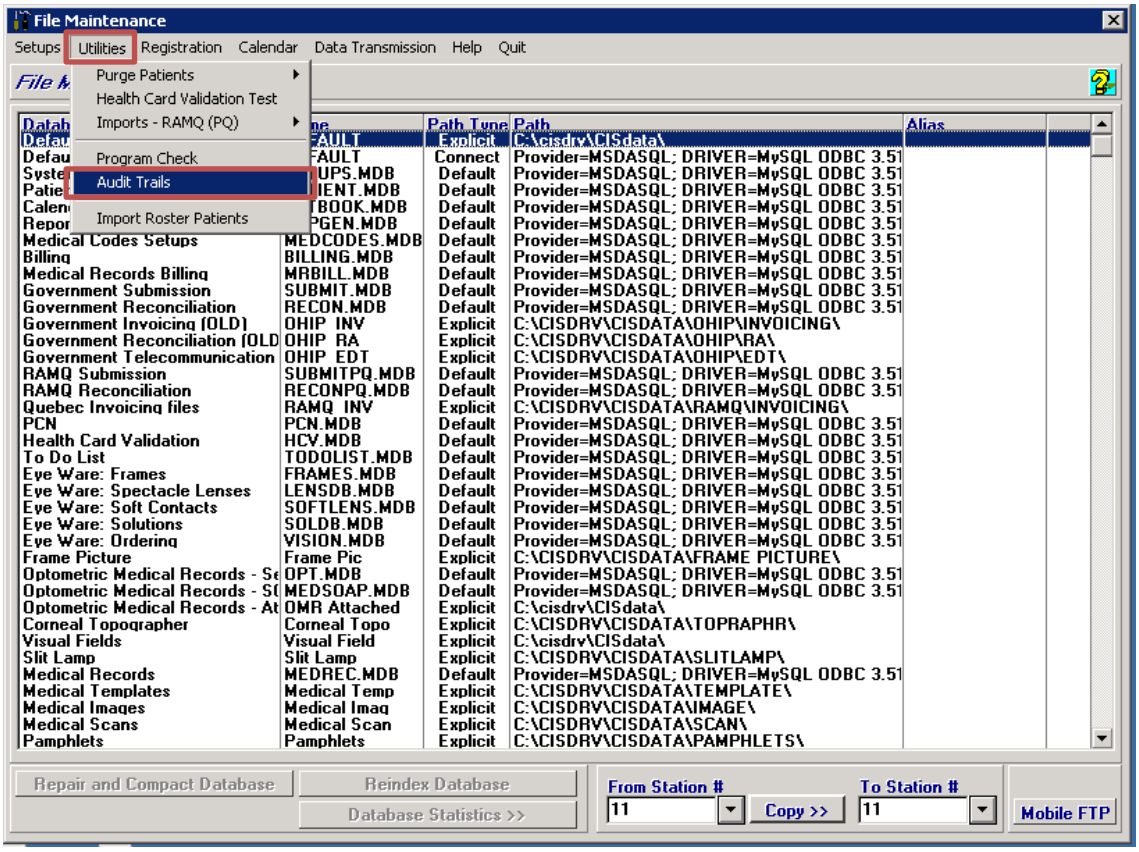




6. On the top toolbar, click **Setups**, then **Files**.



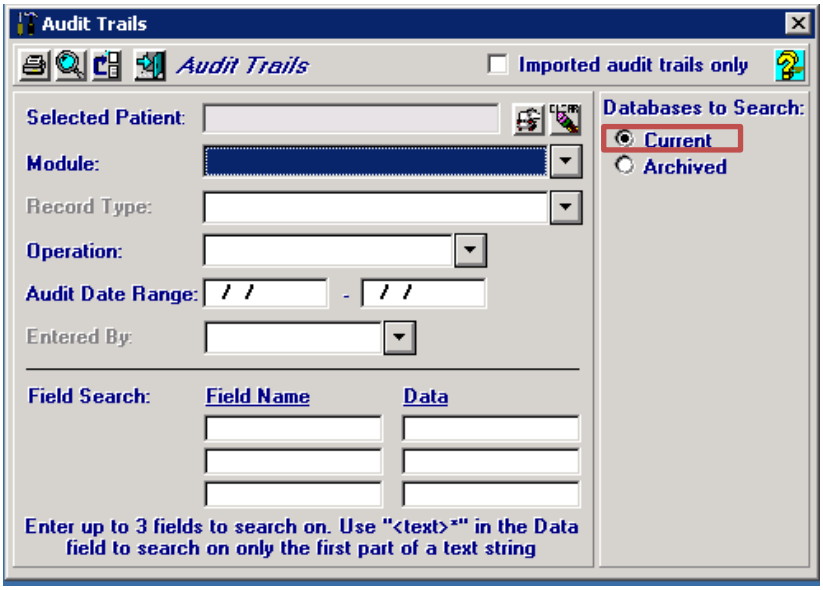
7. The File Maintenance window should appear. On the top toolbar, click **Utilities**, then **Audit Trails**. Refer to page 6 of the guide to audit a specific patient or page 9 to audit a specific user.



Auditing a Specific Patient

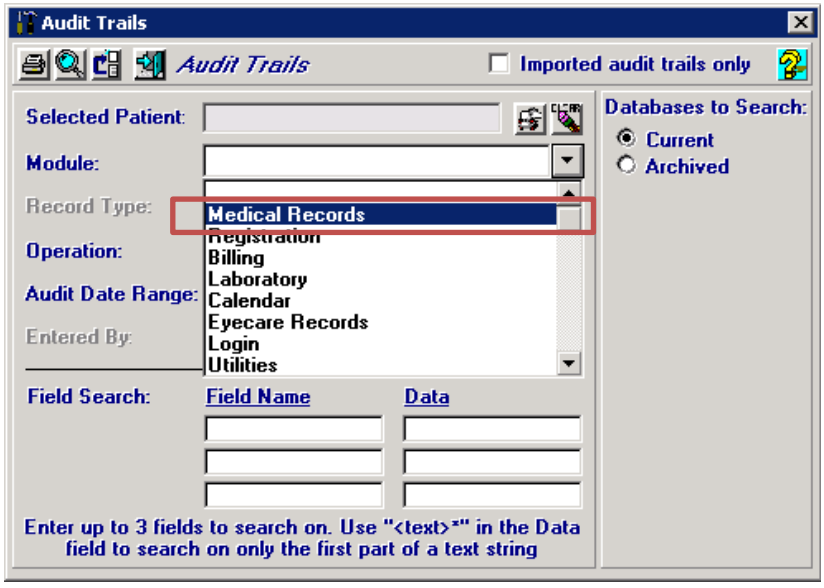
1. Follow the steps in "**Accessing the Audit Trails**" to access the **Audit Trails** window.

2. Make sure that the **Current** option is checked in the **Databases to Search** field.



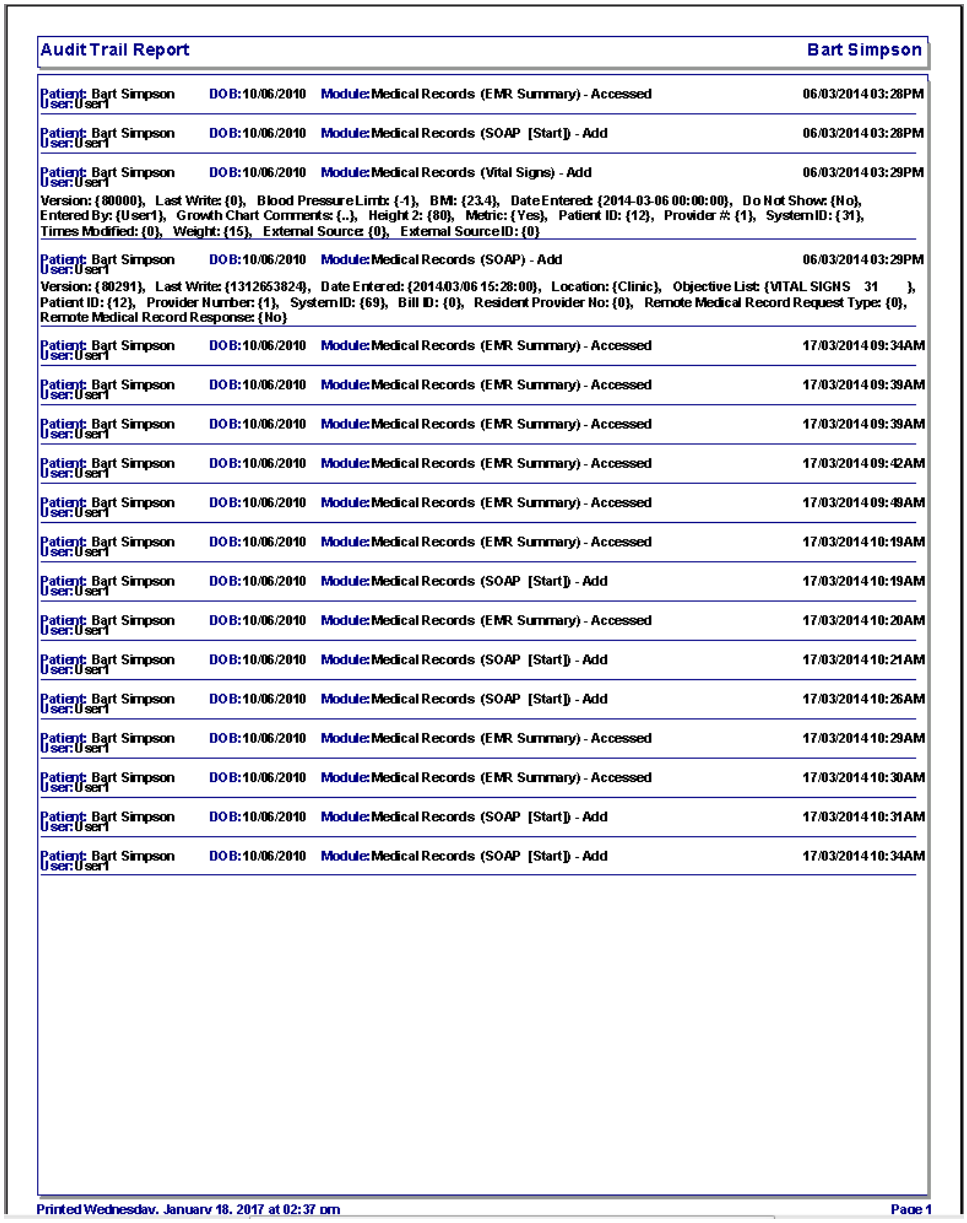
3. Search for a patient by clicking the Patient Search Button () to populate the **Selected Patient** field.

4. Select "**Medical Records**" in the **Module** field.



5. Type in a Start Date (dd/mm/yyyy) and End Date (dd/mm/yyyy) in the **Audit Date Range** fields to specify a certain time period. Alternatively, double click the **Date Range** fields to open up a calendar.
6. Click on the printer button () to generate the Audit Trail Report.

This patient-specific Audit Trail Report records all the activities performed by every user within the Medical Records module for the patient specified in the search bar for the given time period. Note that the Audit Trail Report can be multiple pages.



Audit Trail Report — **Bart Simpson**

Patient: Bart Simpson DOB:10/06/2010 Module:Medical Records (EMR Summary) - Accessed 06/03/2014 03:28PM
User:User1

Patient: Bart Simpson DOB:10/06/2010 Module:Medical Records (SOAP [Start]) - Add 06/03/2014 03:28PM
User:User1

Patient: Bart Simpson DOB:10/06/2010 Module:Medical Records (Vital Signs) - Add 06/03/2014 03:29PM
User:User1
Version: {80000}, Last Write: {0}, Blood Pressure Limb: {-1}, BMI: {23.4}, Date Entered: {2014-03-06 00:00:00}, Do Not Show: {No}, Entered By: {User1}, Growth Chart Comments: {..}, Height 2: {80}, Metric: {Yes}, Patient ID: {12}, Provider #: {1}, System ID: {31}, Times Modified: {0}, Weight: {15}, External Source: {0}, External Source ID: {0}

Patient: Bart Simpson DOB:10/06/2010 Module:Medical Records (SOAP) - Add 06/03/2014 03:29PM
User:User1
Version: {80291}, Last Write: {1312653824}, Date Entered: {2014/03/06 15:28:00}, Location: {Clinic}, Objective List: {VITAL SIGNS 31 }, Patient ID: {12}, Provider Number: {1}, System ID: {69}, Bill ID: {0}, Resident Provider No: {0}, Remote Medical Record Request Type: {0}, Remote Medical Record Response: {No}

Patient: Bart Simpson DOB:10/06/2010 Module:Medical Records (EMR Summary) - Accessed 17/03/2014 09:34AM
User:User1

Patient: Bart Simpson DOB:10/06/2010 Module:Medical Records (EMR Summary) - Accessed 17/03/2014 09:39AM
User:User1

Patient: Bart Simpson DOB:10/06/2010 Module:Medical Records (EMR Summary) - Accessed 17/03/2014 09:39AM
User:User1

Patient: Bart Simpson DOB:10/06/2010 Module:Medical Records (EMR Summary) - Accessed 17/03/2014 09:42AM
User:User1

Patient: Bart Simpson DOB:10/06/2010 Module:Medical Records (EMR Summary) - Accessed 17/03/2014 09:49AM
User:User1

Patient: Bart Simpson DOB:10/06/2010 Module:Medical Records (EMR Summary) - Accessed 17/03/2014 10:19AM
User:User1

Patient: Bart Simpson DOB:10/06/2010 Module:Medical Records (SOAP [Start]) - Add 17/03/2014 10:19AM
User:User1

Patient: Bart Simpson DOB:10/06/2010 Module:Medical Records (EMR Summary) - Accessed 17/03/2014 10:20AM
User:User1

Patient: Bart Simpson DOB:10/06/2010 Module:Medical Records (SOAP [Start]) - Add 17/03/2014 10:21AM
User:User1

Patient: Bart Simpson DOB:10/06/2010 Module:Medical Records (SOAP [Start]) - Add 17/03/2014 10:26AM
User:User1

Patient: Bart Simpson DOB:10/06/2010 Module:Medical Records (EMR Summary) - Accessed 17/03/2014 10:29AM
User:User1

Patient: Bart Simpson DOB:10/06/2010 Module:Medical Records (EMR Summary) - Accessed 17/03/2014 10:30AM
User:User1

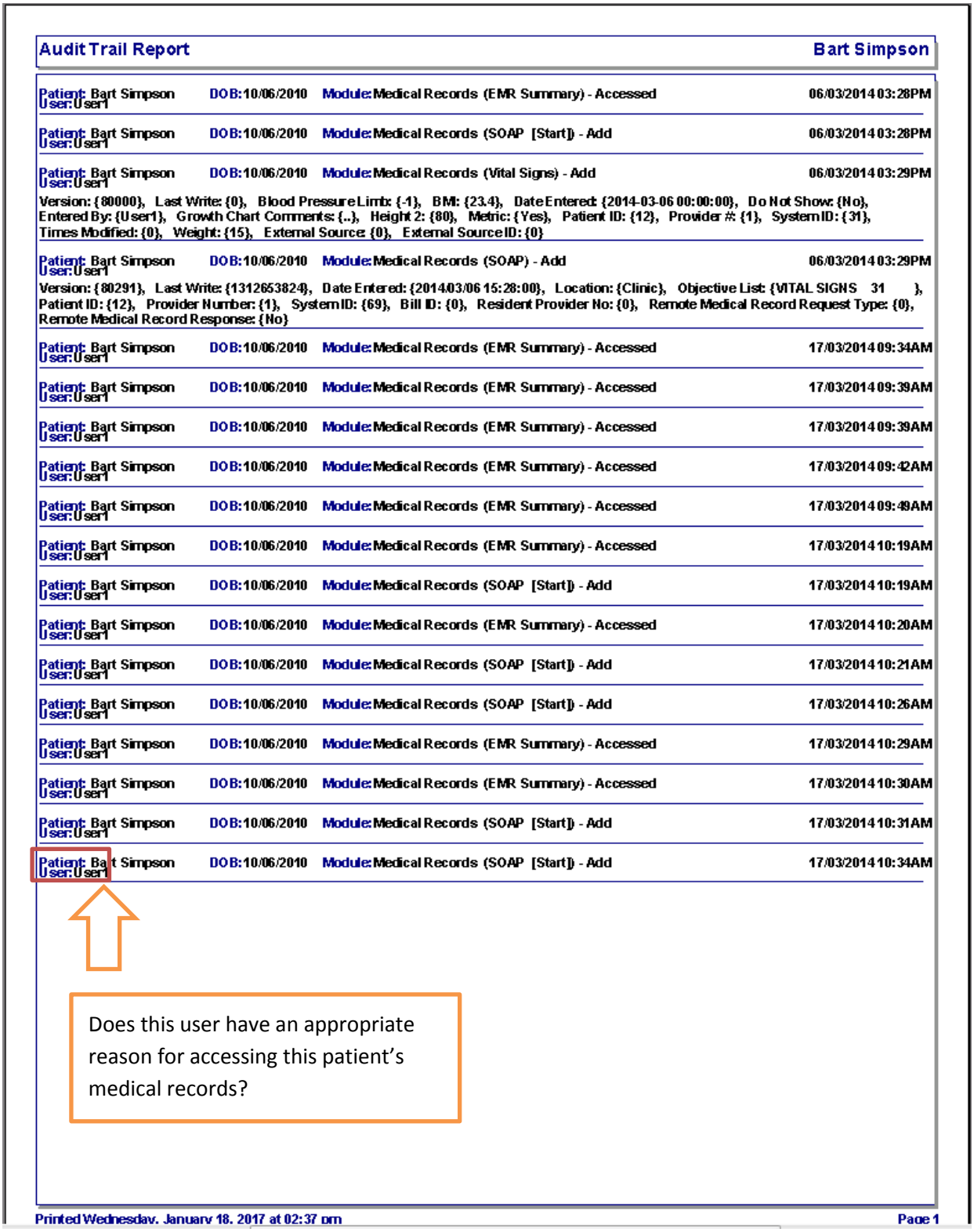
Patient: Bart Simpson DOB:10/06/2010 Module:Medical Records (SOAP [Start]) - Add 17/03/2014 10:31AM
User:User1

Patient: Bart Simpson DOB:10/06/2010 Module:Medical Records (SOAP [Start]) - Add 17/03/2014 10:34AM
User:User1

Printed Wednesday, January 18, 2017 at 02:37 pm — Page 1

Use:

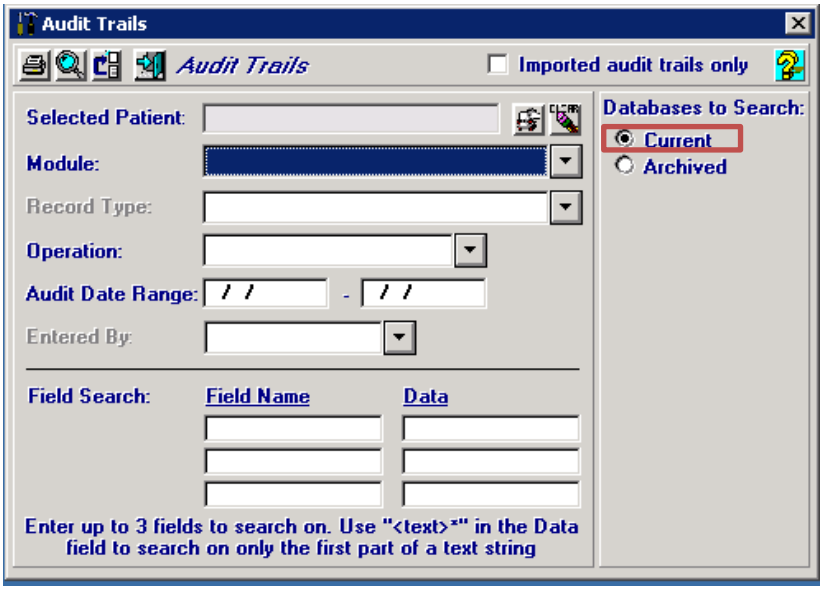
Verify that the appropriate users are accessing a certain patient's files.



Auditing User-specific Activity

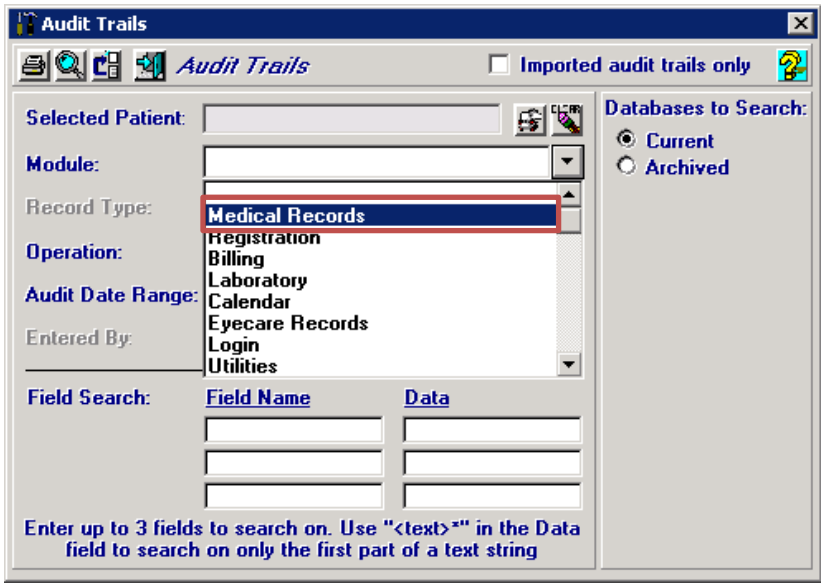
1. Follow the steps in "**Accessing the Audit Trails**" to access the **Audit Trails** window.

2. Make sure that the **Current** option is checked in the **Databases to Search** field.



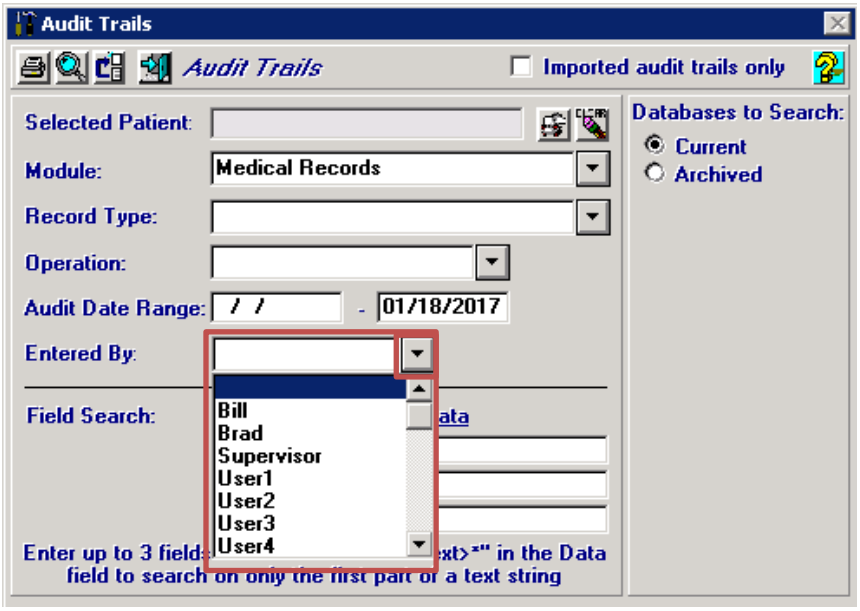
3. Click on the magnifier glass button () to make the **Entered By** field accessible.

4. Select "**Medical Records**" in the **Module** field.



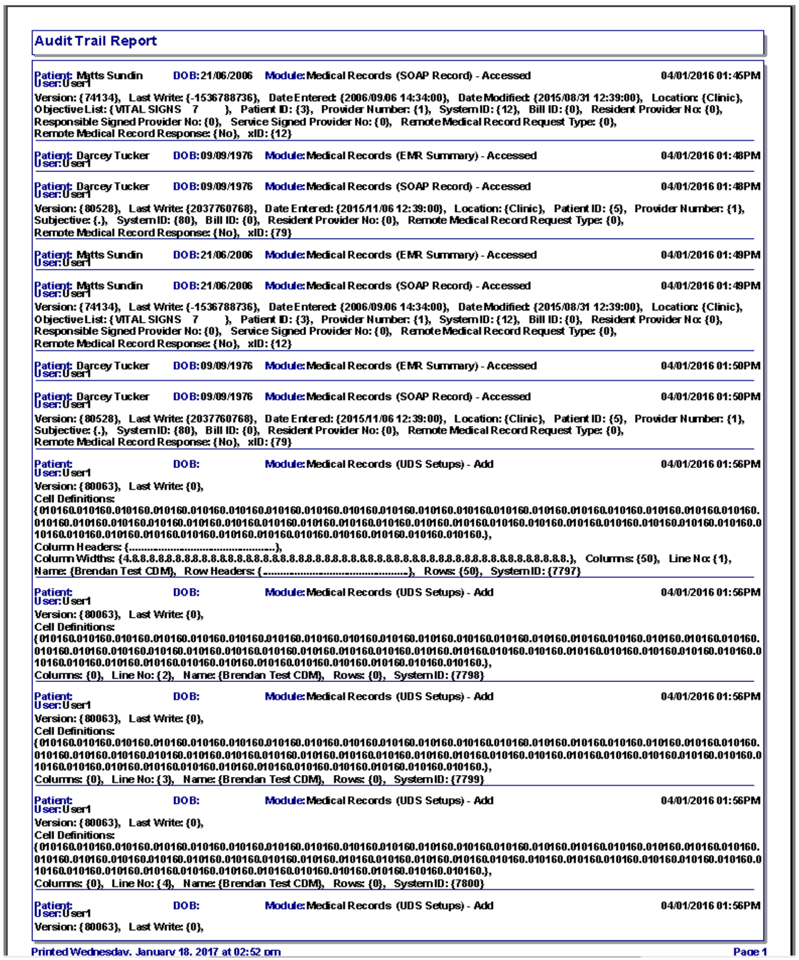
5. Type in a Start Date (dd/mm/yyyy) and End Date (dd/mm/yyyy) in the **Audit Date Range** fields to specify a certain time period. Alternatively, double click the **Date Range** fields to open up a calendar.

6. Select a User from the dropdown menu in the **Entered By** field.



7. Click on the printer button () to generate the Audit Trail Report.

This user-specific Audit Trail records all the activities performed by the user specified in the search bar within the Medical Records module for the given time period. Note that the Audit Trail Report can be multiple pages.



Audit Trail Report

Patient: Matts Sundin DOB: 21/06/2006 Module: Medical Records (SOAP Record) - Accessed 04/01/2016 01:45PM
User: User1
Version: {74134}, Last Write: {-1536788736}, Date Entered: {2006/09.06 14:34:00}, Date Modified: {2015/08/31 12:39:00}, Location: {Clinic}, Objective List: {VITAL SIGNS 7 }, Patient ID: {3}, Provider Number: {1}, System ID: {12}, Bill ID: {0}, Resident Provider No: {0}, Responsible Signed Provider No: {0}, Service Signed Provider No: {0}, Remote Medical Record Request Type: {0}, Remote Medical Record Response: {No}, xID: {12}

Patient: Darcey Tucker DOB: 09/09/1976 Module: Medical Records (EMR Summary) - Accessed 04/01/2016 01:48PM
User: User1

Patient: Darcey Tucker DOB: 09/09/1976 Module: Medical Records (SOAP Record) - Accessed 04/01/2016 01:48PM
User: User1
Version: {80528}, Last Write: {2037760768}, Date Entered: {2015/11/06 12:39:00}, Location: {Clinic}, Patient ID: {5}, Provider Number: {1}, Subjective: {.}, System ID: {80}, Bill ID: {0}, Resident Provider No: {0}, Remote Medical Record Request Type: {0}, Remote Medical Record Response: {No}, xID: {79}

Patient: Matts Sundin DOB: 21/06/2006 Module: Medical Records (EMR Summary) - Accessed 04/01/2016 01:49PM
User: User1

Patient: Matts Sundin DOB: 21/06/2006 Module: Medical Records (SOAP Record) - Accessed 04/01/2016 01:49PM
User: User1
Version: {74134}, Last Write: {-1536788736}, Date Entered: {2006/09.06 14:34:00}, Date Modified: {2015/08/31 12:39:00}, Location: {Clinic}, Objective List: {VITAL SIGNS 7 }, Patient ID: {3}, Provider Number: {1}, System ID: {12}, Bill ID: {0}, Resident Provider No: {0}, Responsible Signed Provider No: {0}, Service Signed Provider No: {0}, Remote Medical Record Request Type: {0}, Remote Medical Record Response: {No}, xID: {12}

Patient: Darcey Tucker DOB: 09/09/1976 Module: Medical Records (EMR Summary) - Accessed 04/01/2016 01:50PM
User: User1

Patient: Darcey Tucker DOB: 09/09/1976 Module: Medical Records (SOAP Record) - Accessed 04/01/2016 01:50PM
User: User1
Version: {80528}, Last Write: {2037760768}, Date Entered: {2015/11/06 12:39:00}, Location: {Clinic}, Patient ID: {5}, Provider Number: {1}, Subjective: {.}, System ID: {80}, Bill ID: {0}, Resident Provider No: {0}, Remote Medical Record Request Type: {0}, Remote Medical Record Response: {No}, xID: {79}

Patient: DOB: Module: Medical Records (UDS Setups) - Add 04/01/2016 01:56PM
User: User1
Version: {80063}, Last Write: {0},
Cell Definitions:
{010160.},
Column Headers: {...},
Column Widths: {4.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.8.}, Columns: {50}, Line No: {1}, Name: {Brendan Test CDM}, Row Headers: {...}, Rows: {50}, System ID: {7797}

Patient: DOB: Module: Medical Records (UDS Setups) - Add 04/01/2016 01:56PM
User: User1
Version: {80063}, Last Write: {0},
Cell Definitions:
{010160.},
Columns: {0}, Line No: {2}, Name: {Brendan Test CDM}, Rows: {0}, System ID: {7798}

Patient: DOB: Module: Medical Records (UDS Setups) - Add 04/01/2016 01:56PM
User: User1
Version: {80063}, Last Write: {0},
Cell Definitions:
{010160.},
Columns: {0}, Line No: {3}, Name: {Brendan Test CDM}, Rows: {0}, System ID: {7799}

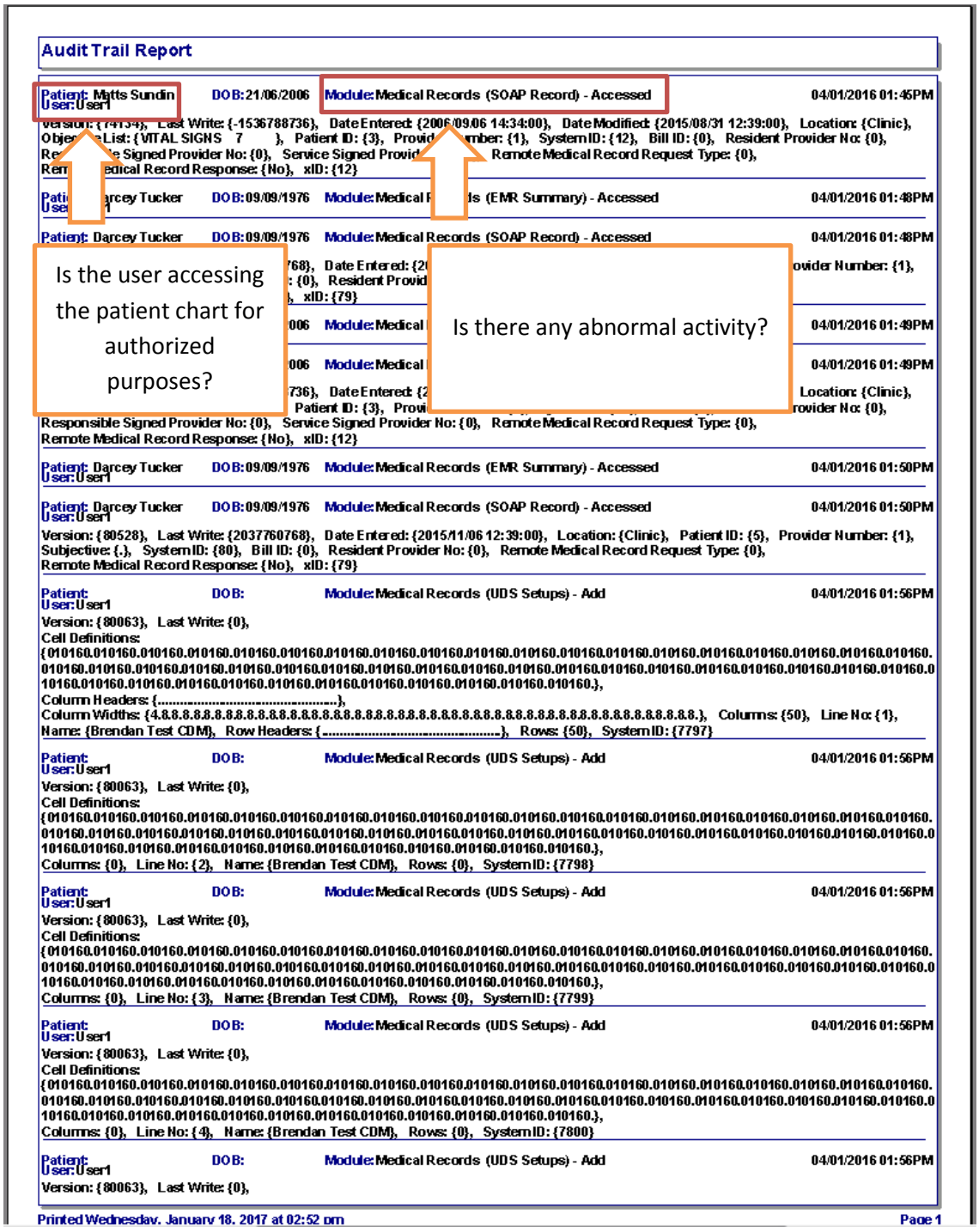
Patient: DOB: Module: Medical Records (UDS Setups) - Add 04/01/2016 01:56PM
User: User1
Version: {80063}, Last Write: {0},
Cell Definitions:
{010160.},
Columns: {0}, Line No: {4}, Name: {Brendan Test CDM}, Rows: {0}, System ID: {7800}

Patient: DOB: Module: Medical Records (UDS Setups) - Add 04/01/2016 01:56PM
User: User1
Version: {80063}, Last Write: {0},

Printed Wednesday, January 18, 2017 at 02:52 pm Page 1

Use:

Verify that the user is accessing records of patients for authorized purposes.



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 P&P, please contact your Quality Improvement Decision Support Specialist (QIDSS).

Appendix

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
- 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:

[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

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: