

2017

Accuro EMR Privacy Audit Guide



Hamilton Family Health Team

Better care, together.

Joshua Tseng, 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 Accuro 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

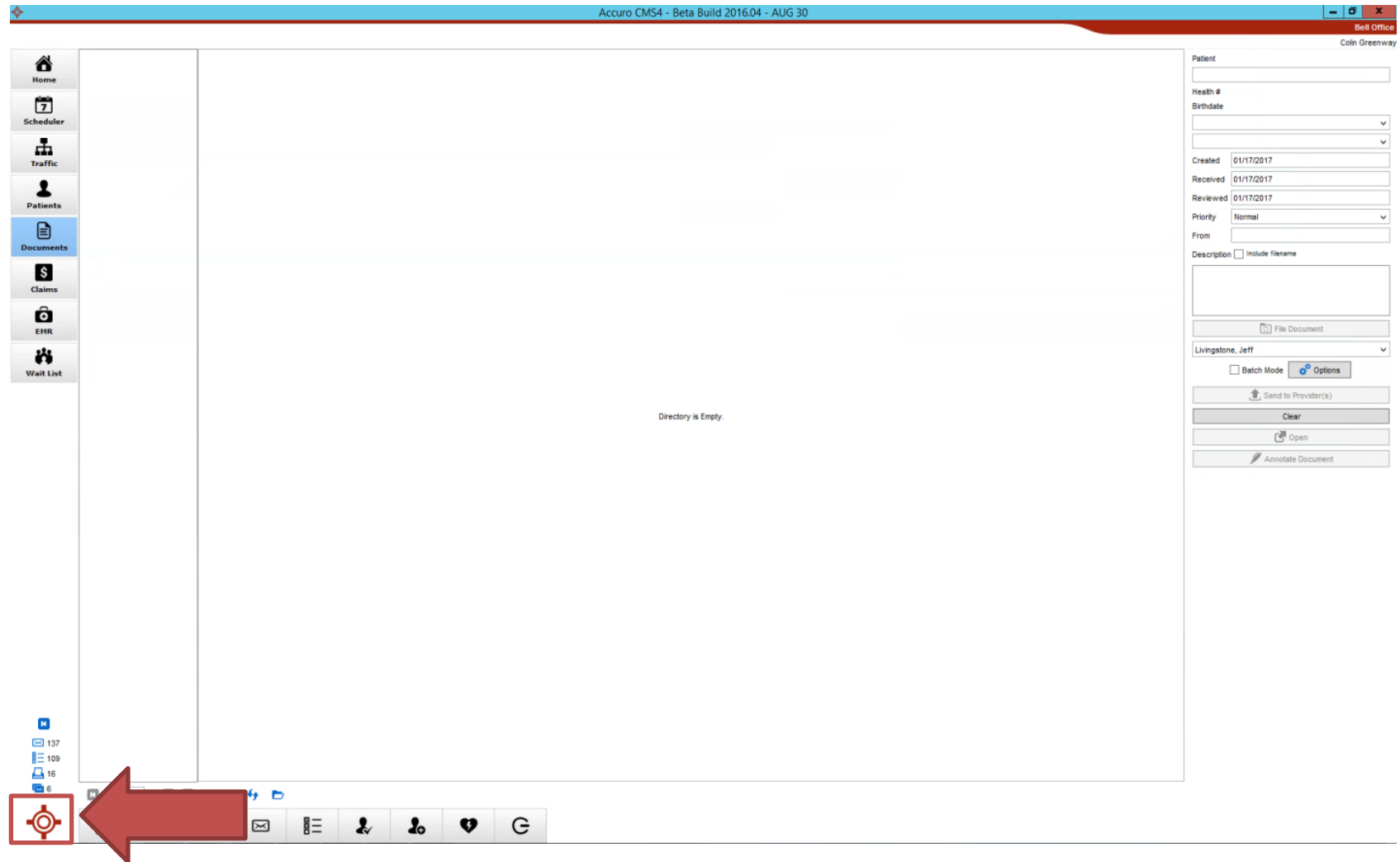
There are several types of audits that you can run in the Accuro EMR. This guide will focus on two types of audits: one that monitors the activity that has occurred in a particular patient's chart, and one that logs specific user activity:

Who/What	Report Type	Page No.
General setup instructions	Accessing the Audit Logs	3
Specific patient audit logs	Auditing a Specific Patient	6
Specific user activity audit logs	Auditing User-specific Activity	8
What to do if you suspect suspicious activity		10
Assistance and contacts		10
Appendix 1.1	HFHT Privacy Breach Protocol	11
Appendix 1.2	Audit Tracking Worksheet	14

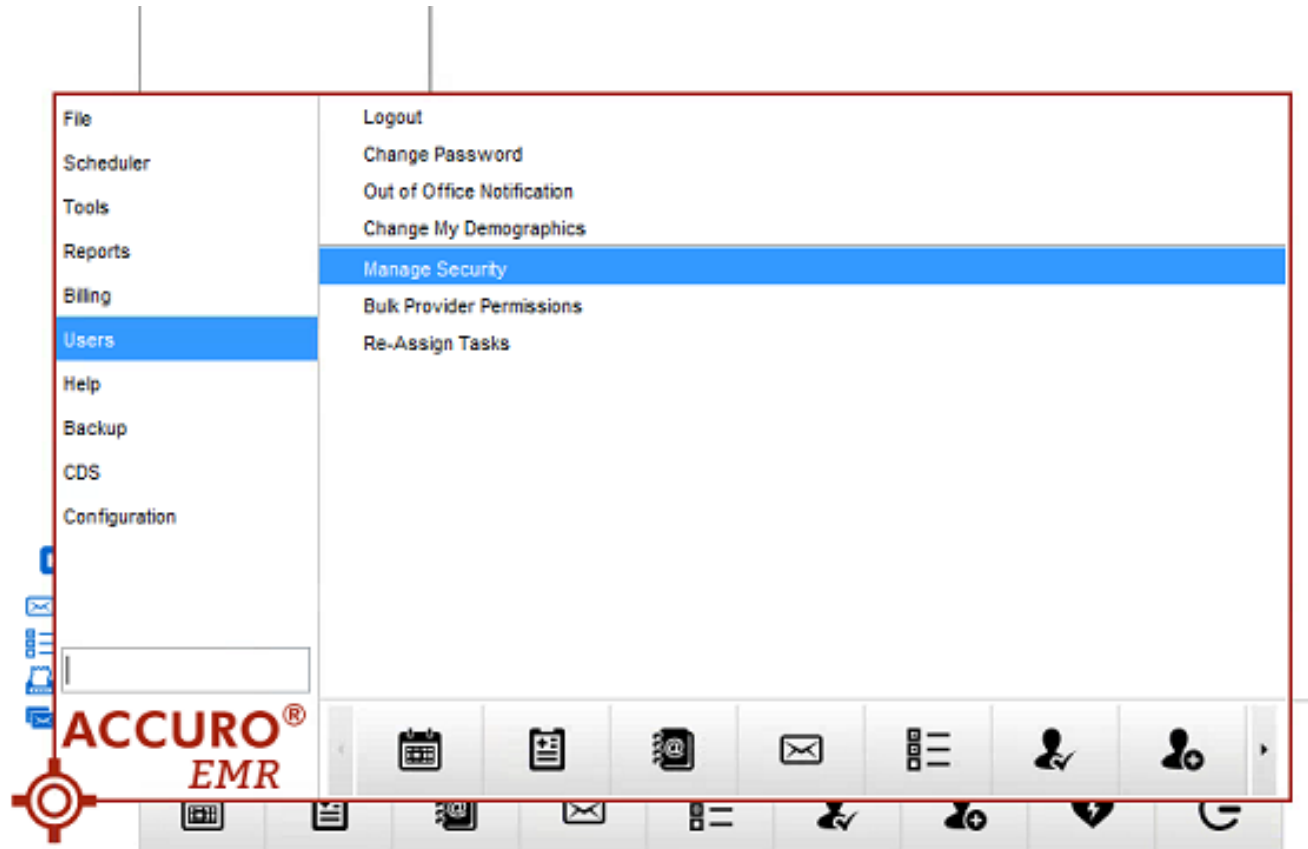
It is recommended that a process for conducting regular audits be established. Auditing specific patients who are more likely to be targets of snooping should be done at least once annually; however, more frequent audits will decrease the amount of records to review and may help make audits more manageable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

Accessing Audit Logs

1. Click the ACCURO logo at the bottom left corner of the program screen. Alternatively, press the **Alt** button on your keyboard.



2. Click **Users**, and select **Manage Security**. The **Manage Security** window will appear.



3. Select the **Audit Logs** tab on the left-hand toolbar. Refer to page 6 to audit a specific patient or skip to page 8 to audit a specific user

The screenshot displays the 'Manage Security' application window. The title bar reads 'Manage Security'. On the left, a vertical toolbar contains several menu items: Roles, Offices, Templates, Users, Feature Access, Notifications, System Settings, **Audit Logs** (highlighted with a red box), Admin Delete, Reports, System Information, and Active Users. The main content area is titled 'Audit Logs' and includes the following elements:

- Date Range:** 01/17/2017 to 01/17/2017, with a print icon and checkboxes for 'Group by Activity' and 'Include Access Logs'.
- Filters:** Activity (--All--), User (--All--), User Demographics Name (--All--), and Role (--All--).
- Options:** A checkbox for 'Patient' and a 'Comments' text input field.
- Activities:** A tabbed interface with 'Activities' and 'Archive' tabs.
- Table:** A table with columns: Trans. ID, Date/Time, User, User Name, Role, Activity, Patient, and two columns labeled 'C...'. A 'List Results' button is located to the right of the table.
- Footer:** A 'Close' button is located at the bottom right of the window.

Auditing a Specific Patient

1. Follow the steps in “**Accessing Audit Logs**” to access the **Audit Logs** tab.
2. Type in a Start Date (mm/dd/yyyy) and End Date (mm/dd/yyyy) in the **Date Range** fields to specify a certain time period. Alternatively, double click the **Date Range** fields to open up a calendar.
3. Check the **Group by Activity** checkbox if you want similar activities kept together.
4. Check the **Patient** checkbox, and type in the patient name in the corresponding field.
5. Click **List Results**.
6. An audit log will appear in the box below the search fields. This patient-specific log records all the activities performed by every user for the patient specified in the search bar for the given time period.

The screenshot shows the 'Manage Security' application window. The 'Audit Logs' tab is active. The search criteria are as follows:

- Date Range: 01/17/2017 to 01/17/2017
- Activity: --All--
- User: --All--
- User Demographics Name: --All--
- Patient: Patient
- Role: --All--

The 'List Results' button is highlighted in the bottom right corner of the main area. The table below the search fields is currently empty.

Trans. ID	Date/Time	User	User Name	Role	Activity	Patient	C...	C...
-----------	-----------	------	-----------	------	----------	---------	-----	-----	------	------

Use:

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

Manage Security

Audit Logs

Date Range: 03/28/2016 to 03/28/2017 Group by Activity Include Access Logs

Activity: --All-- User: --All-- User Demographics Name: --All--

Patient: Test, Test Role: --All--

Comments:

Activities: Archive

Trans...	Date/Time	User	User Name	Role	Activity	Patient	PHN	Pati...	Comm...	Comp...
71413	11/09/2016 1:33 PM	accurosales1		[Office ID - 18227: Physician]	View Chart	Test, Test	99999	1123...	View E...	cts54/1...
71414	11/09/2016 1:33 PM	accurosales1		[Office ID - 18227: Physician]	View Medical Summary	Test, Test	99999	1123...	Viewed...	cts54/1...
71415	11/09/2016 1:33 PM	accurosales1		[Office ID - 18227: Physician]	View Chart	Test, Test				
71416	11/09/2016 1:33 PM	accurosales1		[Office ID - 18227: Physician]	Add Prescription	Test, Test				
71431	11/09/2016 3:49 PM	accurosales1		[Office ID - 18227: Physician]	View Chart	Test, Test				
71432	11/09/2016 3:49 PM	accurosales1		[Office ID - 18227: Physician]	View Medical Summary	Test, Test				
71433	11/09/2016 3:50 PM	accurosales1		[Office ID - 18227: Physician]	Added Form	Test, Test				
71434	11/09/2016 3:50 PM	accurosales1		[Office ID - 18227: Physician]	View Chart	Test, Test	99999	1123...	View E...	cts50/1...
71435	11/09/2016 3:50 PM	accurosales1		[Office ID - 18227: Physician]	View Medical Summary	Test, Test	99999	1123...	Viewed...	cts50/1...
71440	11/09/2016 3:55 PM	accurosales1		[Office ID - 18227: Physician]	View Chart	Test, Test	99999	1123...	View E...	CTS41/...
71441	11/09/2016 3:55 PM	accurosales1		[Office ID - 18227: Physician]	View Medical Summary	Test, Test	99999	1123...	Viewed...	CTS41/...
71454	11/12/2016 9:11 PM	accurosales1		[Office ID - 18227: Physician]	View Chart	Test, Test	99999	1123...	View E...	cts56/1...
71455	11/12/2016 9:11 PM	accurosales1		[Office ID - 18227: Physician]	View Medical Summary	Test, Test	99999	1123...	Viewed...	cts56/1...
71456	11/12/2016 9:11 PM	accurosales1		[Office ID - 18227: Physician]	Added Letter	Test, Test	99999	1123...	Added ...	cts56/1...
71457	11/12/2016 9:11 PM	accurosales1		[Office ID - 18227: Physician]	View Chart	Test, Test	99999	1123...	View E...	cts56/1...
71458	11/12/2016 9:12 PM	accurosales1		[Office ID - 18227: Physician]	View Medical Summary	Test, Test	99999	1123...	Viewed...	cts56/1...
71459	11/12/2016 9:12 PM	accurosales1		[Office ID - 18227: Physician]	Updated Letter	Test, Test	99999	1123...	Update...	cts56/1...
71460	11/12/2016 9:12 PM	accurosales1		[Office ID - 18227: Physician]	View Chart	Test, Test	99999	1123...	View E...	cts56/1...
71461	11/12/2016 9:12 PM	accurosales1		[Office ID - 18227: Physician]	View Medical Summary	Test, Test	99999	1123...	Viewed...	cts56/1...
71462	11/12/20			ID - 18227: Physician]	View Chart	Test, Test	99999	1123...	View pr...	cts56/1...
71463	11/12/20			ID - 18227: Physician]	Add Prescription	Test, Test	99999	1123...	Added ...	cts56/1...

Are the users accessing the chart for authorized purposes?

Double click on a row for more details

List Results

Close

Auditing User-specific Activity

1. Follow the steps in “**Accessing Audit Logs**” to access the **Audit Logs** tab.
2. Type in a Start Date (mm/dd/yyyy) and End Date (mm/dd/yyyy) in the **Date Range** fields to specify a certain time period. Alternatively, double click the **Date Range** fields to open up a calendar.
3. Check the **Group by Activity** checkbox if you want similar activities kept together.
4. Click on the **User** field and select an individual based on their username. Alternatively, you may click the **User Demographics Name** field and select an individual by their actual full name.
5. Click **List Results**.
6. An audit log will appear in the box below the search fields. This user-specific log records all the activities performed by the user specified in the search bar in the given time period.

The screenshot shows the 'Manage Security' application window with the 'Audit Logs' tab selected. The search filters are as follows:

- Date Range: 01/17/2017 to 01/17/2017
- Activity: --All--
- User: --All--
- User Demographics Name: --All--
- Role: --All--

The table below the filters is empty and has the following columns:

Trans. ID	Date/Time	User	User Name	Role	Activity	Patient	C...	C...
-----------	-----------	------	-----------	------	----------	---------	------	------

Use:

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

Manage Security

Audit Logs

Date Range: 03/28/2016 to 03/28/2017

Activity: --All-- User: accurosales1 User Demographics Name: --All--

Role: --All--

Trans...	Date/Time	User	User Name	Role	Activity	Patient	PHN	Patien...	Comment	Computer
64760	04/29/2016 5:53 PM	accurosales1		[Office ID - 18227: Physician]	Login Successful	None				CTS24/172...
64761	04/29/2016 5:55 PM	accurosales1		[Office ID - 18227: Physician]	View Chart	Test, Jackie	11112223...	112468	View EMR ...	CTS24/172...
64762	04/29/2016 5:55 PM	accurosales1		[Office ID - 18227: Physician]	View Medical Summary	Test, Jackie	11112223...	112468		CTS24/172...
64763	04/29/2016 5:56 PM	accurosales1		[Office ID - 18227: Physician]	Added Form	Test, Jackie	11112223...	112468		CTS24/172...
64764	04/29/2016 5:56 PM	accurosales1		[Office ID - 18227: Physician]	View Chart	Test, Jackie	11112223...	112468		CTS24/172...
64765	04/29/2016 5:56 PM	accurosales1		[Office ID - 18227: Physician]	View Medical Summary	Test, Jackie	11112223...	112468		CTS24/172...
64766	04/29/2016 5:57 PM	accurosales1		[Office ID - 18227: Physician]	Added Form	Test, Jackie	11112223...	112468		CTS24/172...
64767	04/29/2016 5:57 PM	accurosales1		[Office ID - 18227: Physician]	View Chart	Test, Jackie	11112223...	112468	Viewed Me...	CTS24/172...
64768	04/29/2016 5:57 PM	accurosales1		[Office ID - 18227: Physician]	View Medical Summary	Test, Jackie	11112223...	112468	Viewed Me...	CTS24/172...
64769	04/29/2016 5:58 PM	accurosales1		[Office ID - 18227: Physician]	View Chart	Test, Jackie	11112223...	112468	Viewed Me...	CTS24/172...
64770	04/29/2016 5:58 PM	accurosales1		[Office ID - 18227: Physician]	View Medical Summary	Test, Jackie	11112223...	112468	Viewed Me...	CTS24/172...
64771	04/29/2016 5:58 PM	accurosales1		[Office ID - 18227: Physician]	View Chart	Test, Jackie	11112223...	112468	View pres...	CTS24/172...
64772	04/29/2016 5:58 PM	accurosales1		[Office ID - 18227: Physician]	Add Presc...	Test, Jackie	11112223...	112468	Added pre...	CTS24/172...
64773	04/29/2016 5:58 PM	accurosales1		[Office ID - 18227: Physician]	Print Rx	Test, Jackie	11112223...	112468	TECTA DR ...	CTS24/172...
64774	04/29/2016 5:58 PM	accurosales1		[Office ID - 18227: Physician]	Logout Succe...	No				CTS24/172...
64775	04/29/2016 5:58 PM	accurosales1		[Office ID - 18227: Physician]	Accuro Exited	No				CTS24/172...
64778	05/02/2016 12:44 PM	accurosales1		[Office ID - 18227: Physician]	Login Succes...	No				cts37/172...
64779	05/02/2016 12:44 PM	accurosales1		[Office ID - 18227: Physician]		No				72...
64780	05/02/2016 12:44 PM	accurosales1		[Office ID - 18227: Physician]		No				72...
64781	05/02/2016 12:45 PM	accurosales1		[Office ID - 18227: Physician]		No				72...
64782	05/02/2016 12:45 PM	accurosales1		[Office ID - 18227: Physician]		No				72...

Is there any abnormal activity?

Is the user accessing these patient charts for authorized purposes?

Double click on a row for more details

Close

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

Appendix 1.1

Hamilton Family Health Team

Privacy Breach Protocol¹

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: