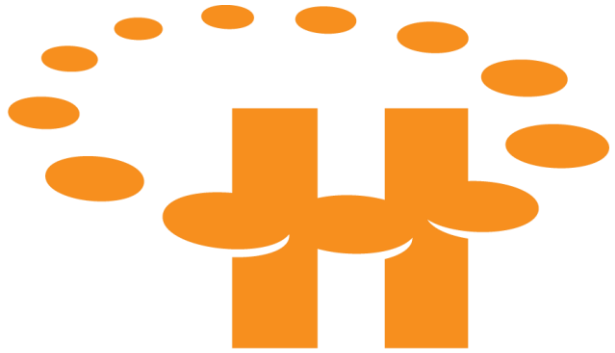
2017

OSCAR EMR Privacy Audit Guide



Hamilton Family Health Team

Better care, together.

Urslin Fevrier-Thomas, 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 in OSCAR 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 8 of this guide can offer some general guidance on next steps.

How to Use This Guide

There are two different types of built-in audit reports that may be run in OSCAR EMR. One report displays the login activity of a user, while the other report is more comprehensive and displays a user's eChart activity as well as their login activity. These reports are identified in OSCAR as Security Log Reports.

In addition to the built-in Security Log reports, an administrator may develop and run SQL queries to determine EMR activity of a user, or eChart activity for specific patients. Knowledge of SQL programming is required to query the EMR database.

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.

Security Logs

Description: All user activity in OSCAR is timestamped and recorded in a security log. The log records activity such as login/log, IP addresses, read, edit, add, update and delete actions performed by a user in patients' eCharts.

The Security Log can be accessed through the Administration link on the main screen in OSCAR.

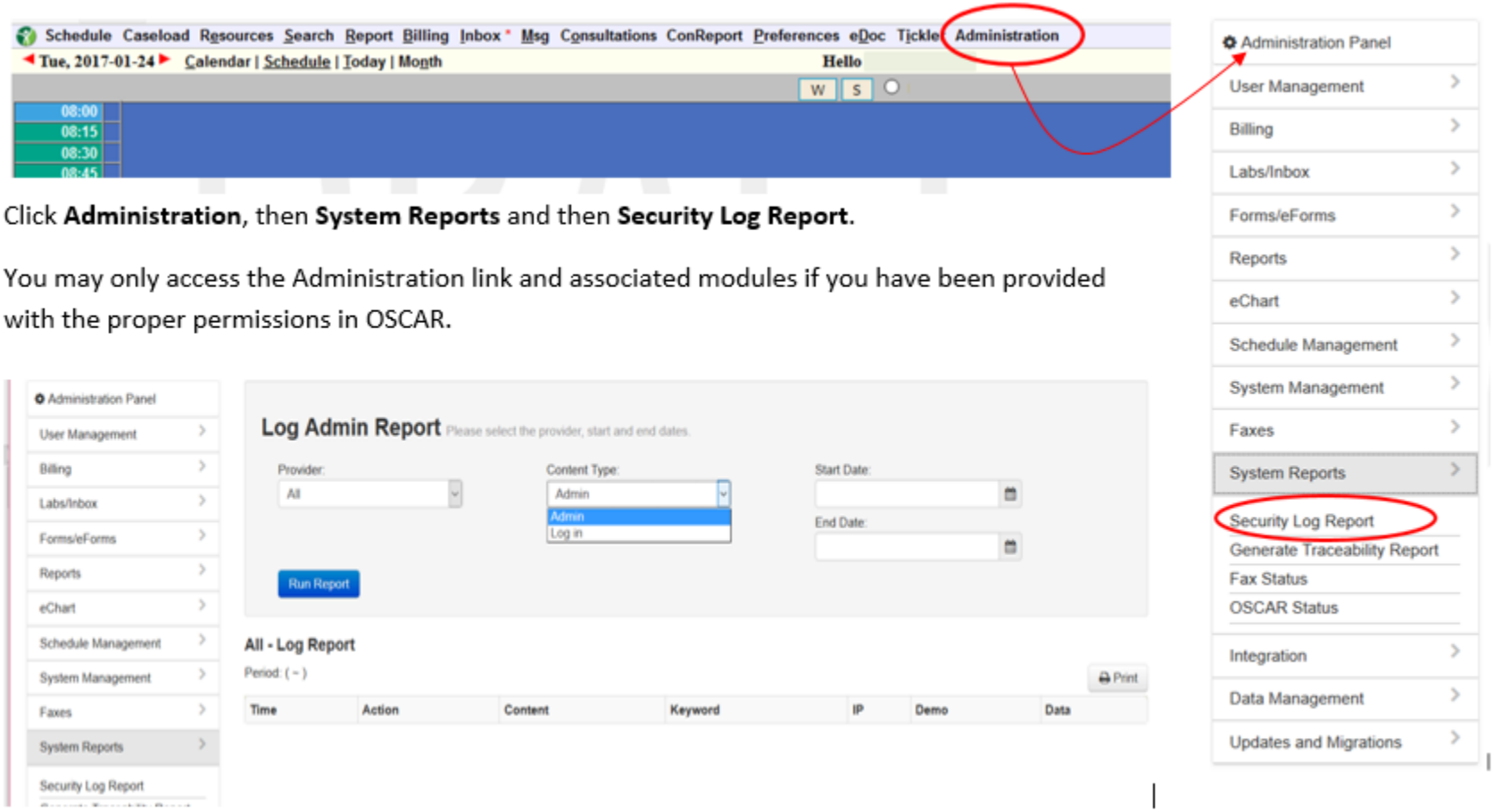
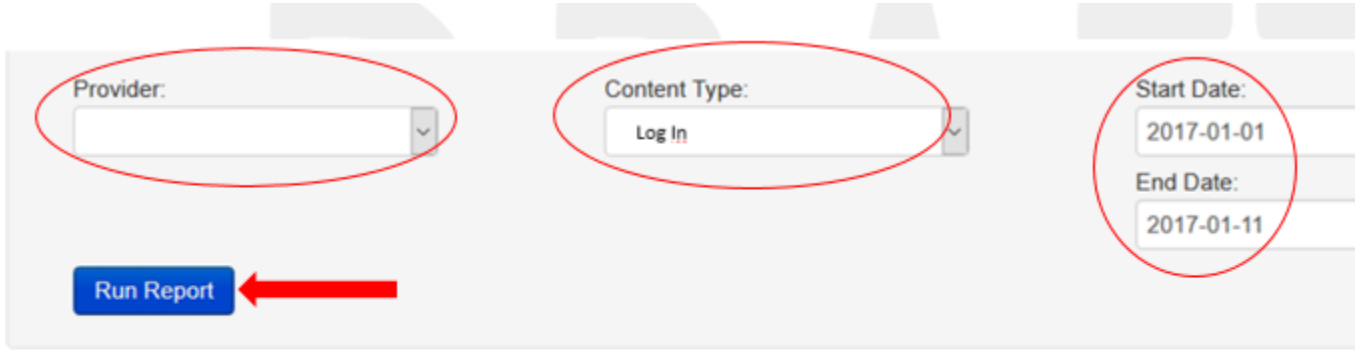


Figure 1

To display the appropriate information, select the **Provider, Content Type** and specific **Start** and **End** dates that you required the information for, and then click on **Run Report**.

Content Type:

- Log In – will display the login activity of a user (Figure 2).
- Admin – will display a comprehensive report of a user's eChart activity as well as their login activity (Figure 3).



[redacted] - Log Report

Period: (2017-01-01 ~ 2017-01-11)

Time	Action	Content	Keyword	IP
2017-01-11 09:11:01.0	log in	login	facilityId=1	[redacted]
2017-01-11 09:11:01.0	log in	login		
2017-01-10 11:03:06.0	log in	login	facilityId=1	
2017-01-10 11:03:06.0	log in	login		

Figure 2

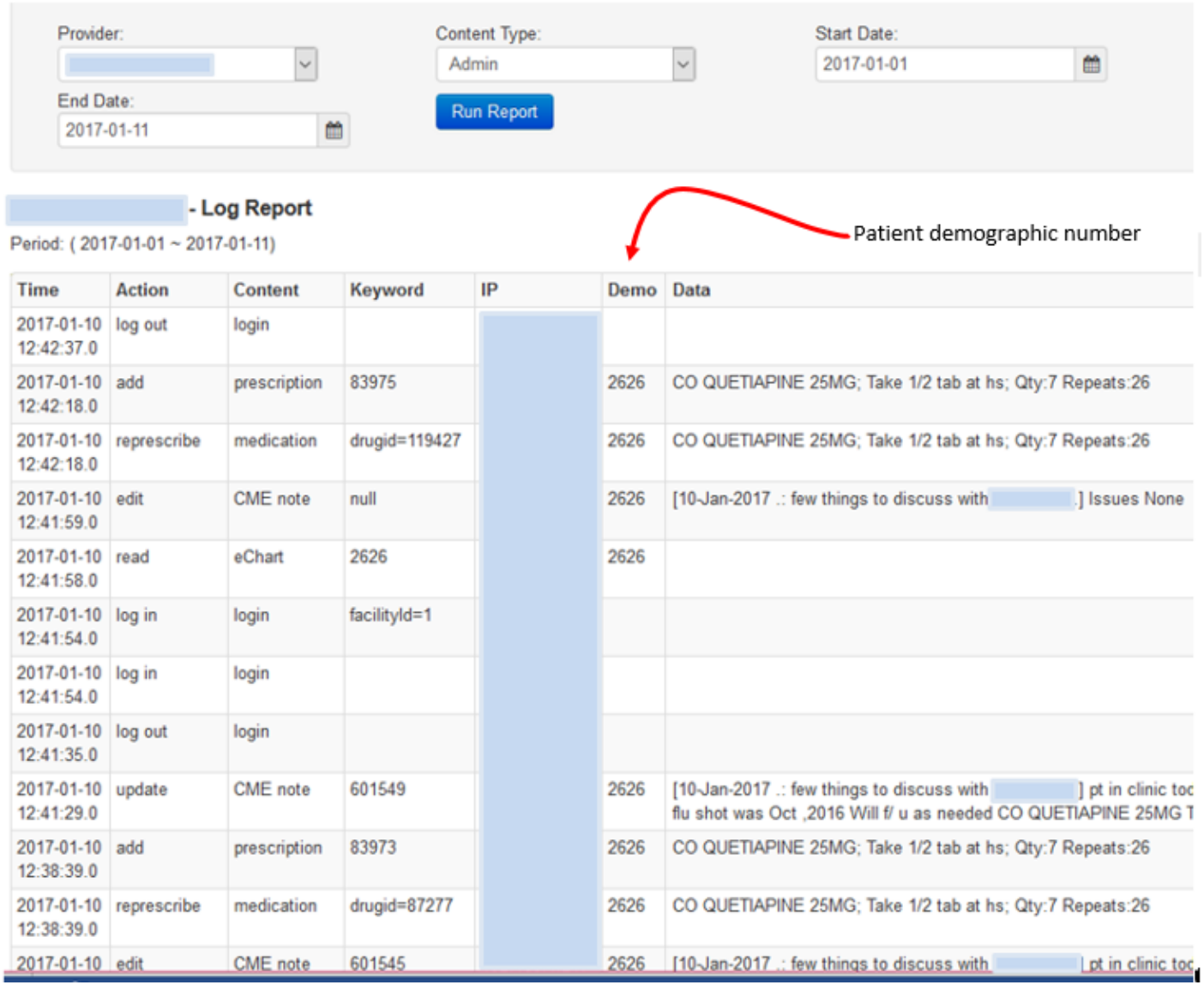
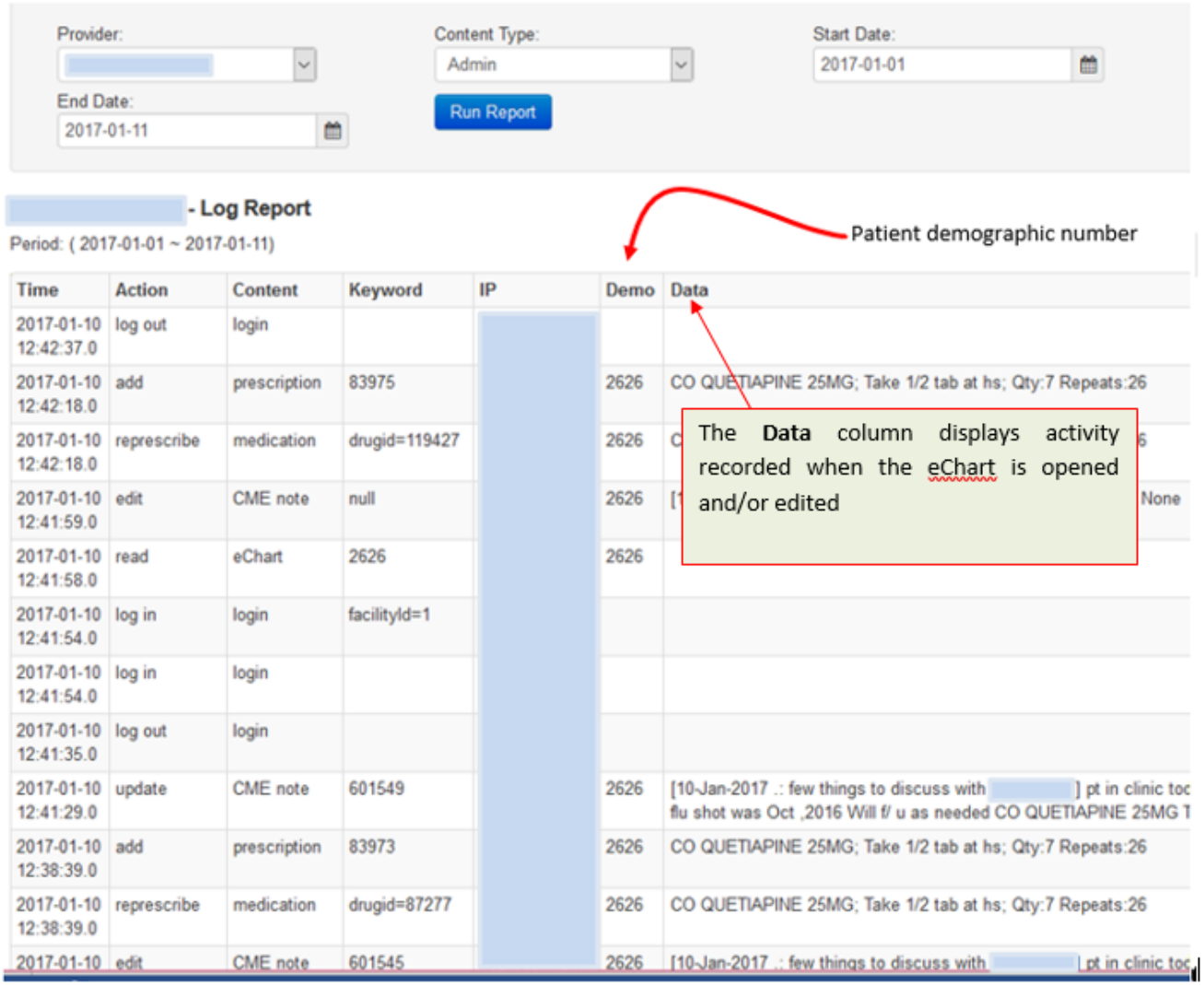

Provider:
Content Type:
Admin
Start Date:
2017-01-01
End Date:
2017-01-11
Run Report
- Log Report
Period: (2017-01-01 ~ 2017-01-11)
Patient demographic number
Time
Action
Content
Keyword
IP
Demo
Data
2017-01-10 12:42:37.0
log out
login
2017-01-10 12:42:18.0
add
prescription
83975
2626
CO QUETIAPINE 25MG; Take 1/2 tab at hs; Qty:7 Repeats:26
2017-01-10 12:42:18.0
represcribe
medication
drugid=119427
2626
CO QUETIAPINE 25MG; Take 1/2 tab at hs; Qty:7 Repeats:26
2017-01-10 12:41:59.0
edit
CME note
null
2626
[10-Jan-2017 .: few things to discuss with] Issues None
2017-01-10 12:41:58.0
read
eChart
2626
2626
2017-01-10 12:41:54.0
log in
login
facilityId=1
2017-01-10 12:41:54.0
log in
login
2017-01-10 12:41:35.0
log out
login
2017-01-10 12:41:29.0
update
CME note
601549
2626
[10-Jan-2017 .: few things to discuss with] pt in clinic toc
flu shot was Oct ,2016 Will f/ u as needed CO QUETIAPINE 25MG T
2017-01-10 12:38:39.0
add
prescription
83973
2626
CO QUETIAPINE 25MG; Take 1/2 tab at hs; Qty:7 Repeats:26
2017-01-10 12:38:39.0
represcribe
medication
drugid=87277
2626
CO QUETIAPINE 25MG; Take 1/2 tab at hs; Qty:7 Repeats:26
2017-01-10
edit
CME note
601545
2626
[10-Jan-2017 .: few things to discuss with] pt in clinic toc

Figure 3

Any of the log reports may be printed or copied and pasted into an Excel file for manipulation.



Time	Action	Content	Keyword	IP	Demo	Data
2017-01-10 12:42:37.0	log out	login				
2017-01-10 12:42:18.0	add	prescription	83975		2626	CO QUETIAPINE 25MG; Take 1/2 tab at hs; Qty:7 Repeats:26
2017-01-10 12:42:18.0	represcribe	medication	drugid=119427		2626	C 6
2017-01-10 12:41:59.0	edit	CME note	null		2626	[1 None
2017-01-10 12:41:58.0	read	eChart	2626		2626	
2017-01-10 12:41:54.0	log in	login	facilityId=1			
2017-01-10 12:41:54.0	log in	login				
2017-01-10 12:41:35.0	log out	login				
2017-01-10 12:41:29.0	update	CME note	601549		2626	[10-Jan-2017 .: few things to discuss with] pt in clinic toc flu shot was Oct ,2016 Will f/ u as needed CO QUETIAPINE 25MG T
2017-01-10 12:38:39.0	add	prescription	83973		2626	CO QUETIAPINE 25MG; Take 1/2 tab at hs; Qty:7 Repeats:26
2017-01-10 12:38:39.0	represcribe	medication	drugid=87277		2626	CO QUETIAPINE 25MG; Take 1/2 tab at hs; Qty:7 Repeats:26
2017-01-10	edit	CME note	601545		2626	[10-Jan-2017 .: few things to discuss with pt in clinic toc

Figure 4

eChart Activity for a Specific Patient

Although the Security Logs may be used to identify activity in OSCAR, data manipulation would be required to filter for specific patients.

To display security log reports by patient, an SQL query would have to be developed and run in the Administration section of OSCAR. Please contact your QIDS Specialist to install and run the additional SQL queries.

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: