# Audit and Monitoring Guidelines for Trustees

Office of the
Saskatchewan Information
and Privacy Commissioner

eHealth
Saskatchewan

## Introduction

Auditing practices are necessary to safeguard personal health information (PHI). Section 16 of *The Health Information Protection Act* (HIPA) requires trustees to put administrative, technical and physical safeguards in place to protect PHI against theft, loss and unauthorized access to or to use, disclosure or modification of the information. As such, it is mandatory for trustees to monitor the access of this information by staff within their organization. The purpose of these guidelines is to assist trustees of personal health information in establishing a proactive audit and monitoring program.

As part of its mandate, the office of the Saskatchewan Information and Privacy Commissioner (IPC) undertakes breach of privacy investigations. All too often after conducting an investigation, it is determined that the breach resulted from employee snooping. In the course of each investigation, the IPC will ask whether or not the trustee does routine or proactive auditing. Surprising, the answer is usually no. There are a number of reasons provided as to why this is the case including not knowing what to audit and when.

Though these guidelines focuses on the 'how to' when it comes to auditing, trustees should also prepare for how to handle requests from patients for copies of user logs/records of user activity. For instance, will the print-outs include the specific name of the health care professional that accessed the patient's personal health information? We recommend that you do. Although the information on the print-out relates to an identifiable individual, it would not be considered personal information of the health care professional as is about the job, not the person in his or her personal capacity. Providing access to these types of print-outs will also help trustees to meet its obligations under HIPA to inform patients of disclosures that have occurred without consent (see section 10).

As well, once the patient receives a copy of the print-out, the name may help the individual to determine whether or not the particular data transaction associated with that health care professional is legitimate or not. A number of complaints have been reported to the IPC as a result of patient scrutiny of such reports. In addition to releasing names, after an internal privacy breach investigation, the trustee should develop a position as to whether or not to inform any affected individuals of any employee discipline resulting from snooping.

In terms of authority to disclose this type of information, the Commissioner has a blog and an investigation report that speak to the specifics. Those are found at:

- http://www.oipc.sk.ca/Blog/2015/2015-09-22_Snooping%20When%20Will%20People%20Learn.pdf
- http://www.oipc.sk.ca/Reports/Investigations/HIPA/2015/100-2015.pdf

## Types of Audits

An audit requires a formal process in order to review, examine and compare the history of an electronic system's records of user activity. As such, the process for auditing should use a structured approach, and should end with a conclusive result. It is important to note, that audits may be scheduled to occur regularly or performed at random. The decision to audit could arise from an incident, a monitoring event, business rules, or in response to a complaint.

### *Random Auditing*

Random audits should be used by the trustee to ensure user compliance with provincial and federal legislation, joint services and access policies (JSAP) and with the trustee's internal privacy and security policies. It is the trustee's responsibility to establish a process for conducting random audits of user activity.

The trustee should consider the following when developing a random audit process:

- The individual(s) responsible for conducting random audits of user activity;
- The frequency of random auditing. Where the number of users and the volume of accesses are great, the frequency of monitoring should increase;
- The reasonable number of users to randomly audit each audit cycle; and
- Events that may trigger a focused audit.

### *Focused Auditing*

A focused audit may be initiated if a complaint is made by a staff member or the general public or if a monitoring activity triggers a more in-depth investigation. All suspected incidents should be investigated and reported in accordance with the trustee's incident management policies and procedures.

### *Monitoring*

On the contrary to auditing, monitoring utilizes a less structured process, and involves continuous checks to verify the effectiveness of the process. Monitoring is often done by creating business rules that trigger alerts which identify suspicious patterns of activity or system use, in turn revealing the need for a more focused audit.

## Who Should Audit User Activity?

It is important for a trustee to appoint one or more individuals to be responsible for monitoring the activity of its employees. It is recommended that the appointed individual(s) are familiar with the following:

- Provincial and federal privacy legislation, such as; *The Freedom of Information and Protection of Privacy Act* (FOIP), the *Personal Information Protection and Electronic Documents Act* (PIPEDA), *The Local Authority Freedom of Information and Protection of Privacy Act* (LAFOIP) and HIPA;
- The trustee's privacy and security policies;
- The type of information the system contains and purpose for which it was collected; and
- The type of access associated with each user role.

As well, processes should be established to ensure regular audits are conducted on the individual(s) responsible for monitoring the activity of employees.

## Audit Triggers

During a random audit, there may be events that can trigger a formal, in-depth investigation. Events which could trigger an investigation include, but are not limited to, the following:

- A user has viewed their own record;
- The type of access is not related to the role of the user who made the access (e.g., a pharmacist views information outside their scope of practice);
- A user views a record of an individual who has the same last name as the user;
- The viewed record belongs to an employee of the organization;
- The number of accesses to one particular record is quite high;
- A record has been viewed outside of scheduled working hours;
- A record has been viewed that does not have an appropriate service event to match (e.g., a record from 5 years ago was viewed recently, yet there are no recent visits made by the patient);
- A record has been viewed that is associated with a media event (e.g., records relating to a suspected bioterrorism attack);
- A record has been accessed that is associated with a VIP (e.g., celebrities, board members, politicians); and
- Break-the-glass events (e.g., a user overrides a mask put on an individual's record).

## Training

Trustees should have appropriate agreements in place to ensure that employees are aware of the organization's privacy and security policies and procedures and their responsibility for compliance. As well, employees should receive annual mandatory training to remind them of their obligations and responsibilities to protect personal and personal health information and to access it on a need-to-know basis. It is important that all employees are made aware that monitoring of user's activity will occur without notice.

## Sources Used


Canada Health Infoway. (2012). *Privacy and EHR Information Flows in Canada: Common Understandings of the Pan-Canadian Health Information Privacy Group.* Retrieved from https://www.infoway-inforoute.ca/en/component/edocman/resources/reports/privacy/502-privacy-and-ehr-information-flows-in-canada-version-2-0?Itemid=101

Manitoba Health, Healthy Living and Seniors. (2014). *Guidelines for Records of User Activity (RoUA)*. Retrieved from https://www.gov.mb.ca/health/phia/docs/gfroua.pdf

Saskatchewan Medical Association. (2013). *Privacy and Security Resource Materials for Saskatchewan EMR Physicians: Guidelines, Samples and Templates*. Retrieved from http://www.sma.sk.ca/kaizen/content/files/Reference_Manual_Jan_2013(1).pdf