Chapter 30
eHealth Saskatchewan—Protecting Patient Information in the Saskatchewan Lab Results Repository

1.0 Main Points

eHealth Saskatchewan is responsible for the provincial electronic health records (eHR), and the means by which healthcare providers access the electronic health information.

Electronically sharing health information presents security risks, including potentially inappropriate access to patient information. eHealth is responsible for protecting patient information in Saskatchewan Lab Results Repository (SLRR)—which forms part of the provincial eHR.

By August 2017, eHealth had fully addressed two of the five recommendations originally made in our 2015 audit of protecting patient information in the SLRR.

Since our 2015 audit, eHealth better supported removal of unneeded user access to patient data in electronic health records and enhanced ways to identify inappropriate access to lab results. But, more work remains to protect patient information. eHealth continues to need to:

- Establish a process to confirm access given to SLRR users remains appropriate
- Update its SLRR systems for critical vulnerabilities within a reasonable timeframe
- Follow its password expiry policy for privileged accounts that access SLRR

2.0 Introduction

Our *2015 Report – Volume 1*, Chapter 10 concluded that for the 12-month period ended March 31, 2015, eHealth had effective processes to secure patient information in SLRR other than matters reflected in our five recommendations.

This chapter describes our follow up of management's actions on those five recommendations.

SLRR is one of several repositories that form part of Saskatchewan's electronic health records. Besides lab results, the electronic health records (patient information) include:

- Medication information
- Immunization information
- Discharge summaries
- Medical imaging reports
- Clinical encounters

- Structured medical records
- Chronic disease information [1]

eHealth gives certain health care providers access to this data through eHR Viewer. eHR Viewer is a secure website that authorized health care providers can use to access patient information, no matter where a patient goes for care.[2]

To conduct this audit engagement, we followed the standards for assurance engagements published in the *CPA Canada Handbook – Assurance* (including CSAE 3001). To evaluate eHealth's progress towards meeting our recommendations, we used the relevant criteria from the original audit. eHealth's management agreed with the criteria in the original audit.

We reviewed and assessed related reports, policies, and IT system settings with eHealth officials. We tested a sample of user account requests.

3.0 Status of Recommendations

This section sets out each recommendation including the date on which the Standing Committee on Public Accounts agreed to the recommendation, the status of the recommendation at August 31, 2017, and eHealth's actions up to that date.

eHealth implemented two recommendations and made progress on two of the other three recommendations.

3.1 Reports Developed to Support Detection of Inappropriate Access

> ***We recommended that eHealth Saskatchewan assess risks of inappropriate access to lab results in the Saskatchewan Lab Results Repository and set up alerts to enable timely detection.*** (2015 Report – Volume 1; Public Accounts Committee agreement January 13, 2016)
>
> **Status** – Implemented

Since our 2015 report, eHealth started collaborating with the regional health authorities to help identify risks of potentially inappropriate access to electronic health records.

eHealth continues to monitor instances where a user of eHR Viewer accesses patient data that is masked—meaning the patient has requested that their data only be viewed in special circumstances. eHealth also monitors when users from the Saskatchewan Disease Control Laboratory access non-SLRR data.

In 2016, eHealth started using a new electronic privacy audit and monitoring tool. Working with privacy officers at regional health authorities, they identified risks associated with potentially inappropriate access and eHealth developed related reports. As a result, at October 2017, the tool could generate reports outlining the following:

[1] www.ehealthsask.ca/services/ehr-viewer (16 October 2017).
[2] Ibid.

- Instances when a user of the eHR Viewer has accessed a medical profile of a patient with the same last name
- Trends in the number of patient records accessed in the eHR Viewer on a daily basis compared to expected daily averages
- Patients looked up after discharge

By using these reports, regional health authorities can further analyze the list of potential instances of inappropriate access.

In April 2017, eHealth formed a privacy audit and monitoring working group consisting of eHealth and officials from six regional health authorities. The group is to develop further enhancements to the privacy audit and monitoring tool, and identify specific events to monitor. By October 2017, the group had met several times. Future enhancements will continue to increase the effectiveness of detecting and investigating potential inappropriate access to patient data.

3.2 User Access Removed Timely but Policy Still Required to Confirm Access Periodically

> ***We recommended that eHealth Saskatchewan implement a policy to require prompt removal of user access to eHR Viewer upon request.*** (2015 Report – Volume 1; Public Accounts Committee agreement January 13, 2016)
>
> **Status** – Implemented

eHealth has, through its service level agreements, established a turnaround time for removing eHR Viewer user access once requested.

Service level agreements between eHealth and its clients (e.g., regional health authorities) outline user account request turnaround targets (i.e., five days).

We tested a sample of user access requests and found eHealth processed requests in accordance with its turnaround targets.

> ***We recommended that eHealth Saskatchewan implement a policy to confirm periodically with healthcare organizations that existing users have appropriate access to the Saskatchewan Lab Results Repository through the eHR Viewer.*** (2015 Report – Volume 1; Public Accounts Committee agreement January 13, 2016)
>
> **Status** – Partially Implemented

eHealth began working towards periodically confirming users have appropriate access to SLRR.

In 2015, eHealth provided a list of eHR Viewer users to user account approvers to confirm appropriateness of access. eHealth has since been working on refining the report accuracy, and intends to confirm the list of users in 2017-18 and annually going forward.

Not requiring a periodic review of existing users increases the risk that users who no longer require access continue to have the ability to view confidential patient data.

3.3 Passwords Not Changed Periodically for Accounts with Privileged Access

We recommended that eHealth Saskatchewan follow its password expiry policy for privileged user accounts that access the Saskatchewan Lab Results Repository. (2015 Report – Volume 1; Public Accounts Committee agreement January 13, 2016)

Status – Not Implemented

Contrary to its password expiry policy, eHealth continues to have accounts with privileged access (e.g., system administrator accounts) to SLRR with passwords that do not expire. Users with privileged IT access are able to change systems or data that ordinary users are not. Not using passwords that expire increases the risk that a password may be compromised and/or a system breached.

3.4 Available Security Updates to System Not Applied within a Reasonable Timeframe

We recommended that eHealth Saskatchewan properly configure and update, on a timely basis, its Saskatchewan Lab Results Repository systems for critical vulnerabilities. (2015 Report – Volume 1; Public Accounts Committee agreement January 13, 2016)

Status – Partially Implemented

eHealth has not updated its SLRR systems within a reasonable timeframe. As of August 2017, eHealth has not applied certain updates available since 2012 to its SLRR systems. eHealth did not have a documented risk analysis to explain why it did not do so.

eHealth applies security patches to servers that support SLRR within a reasonable period.

Not updating the SLRR systems within a reasonable period increases the risk of unauthorized access to eHealth's systems and data.