# Chapter 10
# eHealth Saskatchewan—Protecting Patient Information in the Saskatchewan Laboratory Results Repository

## 1.0 Main Points

eHealth Saskatchewan (eHealth) is responsible for the provincial electronic health records (EHR) for patients and for providing healthcare professionals with access to those records. eHealth is creating the provincial EHR by compiling and standardizing key patient data from different regional health authorities and healthcare providers into provincial data repositories. One of these repositories is the Saskatchewan Lab Results Repository (SLRR). SLRR distributes lab results through a website to healthcare professionals.

Electronically sharing information creates security risks, such as unauthorized or inappropriate access to sensitive information. eHealth is responsible for protecting patient information in SLRR.

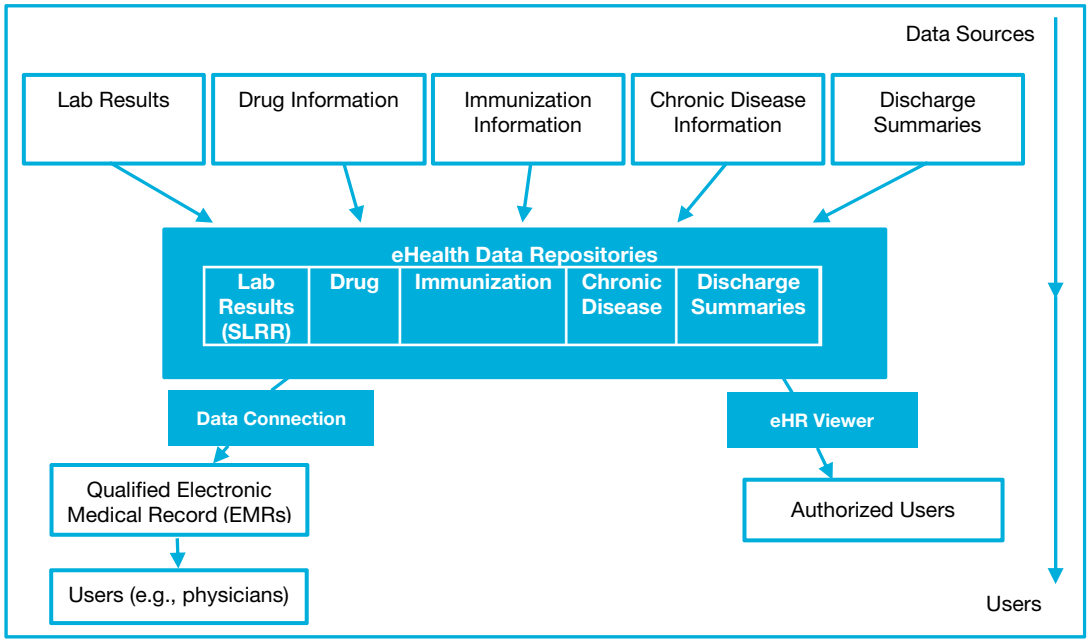
For the 12-month period ended March 31, 2015, eHealth had effective processes to secure patient information in the SLRR except it needs to:

- Set up alerts to enable timely detection of inappropriate access to lab results in SLRR
- Properly update SLRR systems to reduce threat of unauthorized or inappropriate access
- Implement policies to confirm users approved to access SLRR, and require prompt removal of access upon request
- Follow its password expiry policy to force periodic password changes for SLRR privileged user accounts

## 2.0 Introduction

The provincial EHR is a system of comprehensive electronic health records for patients in Saskatchewan that allows the electronic sharing of patient data among healthcare professionals. The provincial EHR is expected to improve patient care and generate healthcare efficiencies. eHealth Saskatchewan (eHealth) is a Treasury Board Crown corporation responsible for developing and implementing the provincial EHR in Saskatchewan. As illustrated in **Figure 1**, the provincial EHR collects patient information (e.g., diagnostic images, lab results, immunization information, drug information) from various computer systems.

**Figure 1—Simplified Overview of Provincial Electronic Health Record**




Source: Adapted from eHealth Information Advisory Committee Terms of Reference.
Note: Shaded boxes are within the control of eHealth.

SLRR is a component of the provincial EHR. The data repository distributes lab results to healthcare professionals that it receives from the 12 regional health authorities'[1] lab systems and the Saskatchewan Disease Control Laboratory.[2]

This chapter reports the results of our audit of eHealth's processes to secure patient information in SLRR.

The **Glossary** in **Section 6.0** defines many of the terms used in this chapter.

## 3.0 Protecting Patient Information in SLRR

SLRR is eHealth's computer system that compiles patient lab information (e.g., results of blood and urine tests) into a centralized data repository. eHealth makes patient information in SLRR available to authorized healthcare professionals through:

- eHR Viewer, eHealth's website, which provides authorized users with read-only access to eHealth's data repositories including SLRR. At March 2015, eHealth had given read-only access to 4,000 healthcare professionals (authorized users).

- A data connection that sends patient data from eHealth's data repositories, including SLRR, to qualified[3] electronic medical record (EMR) systems. EMR

[1] Regional Health Authorities (RHAs) are organizations created by *The Regional Health Services Act* to plan, organize, deliver, and evaluate health services in their respective regions. The 12 RHAs are: Cypress, Five Hills, Heartland, Keewatin Yatthé, Kelsey Trail, Mamawetan Churchill River, Prairie North, Prince Albert Parkland, Regina Qu'appelle, Saskatoon, Sun Country, and Sunrise.
[2] The Saskatchewan Disease Control Laboratory is a branch of the Ministry of Health responsible for identifying, responding to, and preventing illness and disease in Saskatchewan. Its services range from routine testing of water supplies to disease outbreak identification and control.
[3] eHealth supports provincial repository access for three approved EMR systems used in physician offices. EMRs enable physicians to record a patient's medical history.

systems are used by regional health authorities and physician-owned and managed healthcare clinics and offices.

Although many benefits can be achieved by electronically sharing patient information with healthcare professionals, appropriate measures are necessary to keep patient information secure.

Under *The Health Information Protection Act* (HIPA), eHealth is obligated to protect patient information in SLRR. Preventing unauthorized or inappropriate access to sensitive information is increasingly challenging, particularly in the healthcare sector, where the main focus is often on client service delivery. Inadequate security could result in the loss or inappropriate use of patient information (e.g., user looking at patient data not required for their work), corruption or manipulation of patient information, medical identity theft, or system failure. The loss of patient information or system failure could impact the timeliness of patient care. If sensitive patient information were to fall into the wrong hands, public trust in health care could be threatened. A loss of confidence in the provincial eHR could result in decreased use by healthcare professionals, or more patients choosing to mask their patient information, which would reduce the benefits of this investment.

## 4.0 Audit Objective, Scope, Criteria, and Conclusion

The objective of this audit was to assess whether eHealth Saskatchewan had effective processes to secure patient information in the Saskatchewan Lab Results Repository (SLRR) from April 1, 2014 to March 31, 2015.

Given that EMRs reside at physician offices and healthcare clinics and are not owned by eHealth, we did not look at the security of data in those systems.

We examined eHealth's policies, procedures, and agreements and interviewed eHealth staff. We also examined eHealth's controls to secure SLRR, including server patch levels, physical security, and users with privileged access.

To conduct this audit, we followed the standards for assurance engagements published in the *CPA Canada Handbook – Assurance*. To evaluate eHealth's processes, we used criteria based on the work of other auditors and literature listed in the selected references. The criteria are primarily based on the *Trust Services Principles, Criteria, and Illustrations* published by the Chartered Professional Accountants of Canada and the American Institute of Certified Public Accountants. eHealth's management agreed with the criteria (see **Figure 2**).

**Figure 2—Audit Criteria**

To have effective processes to secure patient information in SLRR, eHealth should:

1. **Monitor the system and data**
   - 1.1 Responsibilities to secure the system and data are clearly defined
   - 1.2 Management has approved security policies and procedures
   - 1.3 Management monitors and addresses security risks (e.g., unauthorized or inappropriate access)
2. **Protect the system and data from unauthorized access**
   - 2.1 User access controls protect the system and data from unauthorized or inappropriate access
   - 2.2 Physical security controls protect the system and data from unauthorized access

3. **Make the system and data available for operation**
   - 3.1 System and data backups occur and are tested
   - 3.2 Disaster recovery plans are in place and tested
4. **Maintain the integrity of the system and data**
   - 4.1 Processes to manage the system and data exist and are followed
   - 4.2 Change management processes exist and are followed

**We concluded that, for the period of April 1, 2014 to March 31, 2015, eHealth Saskatchewan had, other than the following, effective processes to secure patient information in the Saskatchewan Lab Results Repository. eHealth needs to:**

- **Assess risks of inappropriate access to lab results in the Saskatchewan Lab Results Repository and set up related alerts to enable timely detection**
- **Implement policies to periodically confirm existing users have appropriate access to the eHR Viewer and require prompt removal of eHR Viewer access upon request**
- **Follow its password expiry policy for Saskatchewan Lab Results Repository privileged user accounts**
- **Properly configure and update, on a timely basis, the Saskatchewan Lab Results Repository systems for critical vulnerabilities**

**Also, as identified in our *2014 Report – Volume 2*, Chapter 7, eHealth needs a complete and tested disaster recovery plan.**

## 5.0 Key Findings and Recommendations

In this section, we set out the criteria (expectations) and our key findings along with related recommendations.

### 5.1 Better Monitoring of User Access Needed

*In order to effectively monitor the SLRR system and data, we expected:*

- *Roles and responsibilities for securing the system to be clear. It is important that information technology (IT) employees (i.e., those who design and maintain an IT system) are segregated from operations (i.e., those who use an IT system for their day-to-day jobs).*
- *Documented IT security policies and procedures to be regularly updated.*
- *SLRR to be monitored for unauthorized and inappropriate access and identified security risks to be addressed in a timely manner*.

eHealth has an effective IT organizational structure for securing SLRR. We found it separated operations from IT delivery and made a security group responsible for periodically assessing the state of its IT security. eHealth also has approved security policies and procedures that outline structured processes for securing IT systems,

including SLRR systems and data. At March 2015, eHealth was carrying out a regular update of its security policies and procedures.

eHealth has a standard Master Data Sharing Agreement with each of the 12 regional health authorities (RHAs) and the Ministry of Health (for the Saskatchewan Disease Control Laboratory). Each of these agreements create a data-sharing relationship, whereby lab results received from RHAs and the Saskatchewan Disease Control Laboratory are amalgamated into SLRR. Through these agreements, eHealth becomes the trustee[4] of the data in SLRR.

To govern decision-making related to SLRR, such as user access, eHealth has created a committee called the eHealth Information Advisory Committee. Membership is comprised of patients, various individuals representing RHAs, and other health organizations (e.g., Saskatchewan College of Physicians and Surgeons, Saskatchewan College of Pharmacists). We found the eHealth Information Advisory Committee meets regularly (i.e., three times in 2014-15).

As previously noted, eHealth makes lab results in SLRR available electronically to authorized healthcare providers through qualified EMRs and the eHR Viewer. See **Section 5.2** for a description of the authorization process.

eHealth has operated eHR Viewer, a website, since 2011 and grants authorized users access to view patient data, including lab results, over the Internet. eHealth tracks what each authorized user views through the eHR Viewer. In January 2015, eHealth developed a system to alert it of potential inappropriate access to patient data (alert system). We found that it had set up the alert system to notify eHealth about two types of potential inappropriate access:

- Any authorized user accessing data that is masked. Patients can request eHealth mask their data in eHR Viewer – meaning their patient data can only be viewed in special circumstances (e.g., in life-threatening situations).

- Authorized users from Saskatchewan Disease Control Laboratory accessing non-SLRR data.

During 2014-15, there were two incidents where eHealth was notified by external parties of potential inappropriate access. After the incidents were reported, eHealth examined logs to determine what was accessed and by whom. The types of system alerts currently used are not sufficient to help identify these types of incidents.

Further alerts could notify eHealth of inappropriate access on a timely basis. For example, eHealth could set up alerts to notify it if a user accesses a large number of patient files within a very short time or from unexpected locations (e.g., outside the user's health region or areas of specialization). Not assessing the need for further types of alerts to identify inappropriate user access increases the risk of not sufficiently securing SLRR data.

[4] *The Health Information Protection Act* defines a trustee as a person or organization who has custody or control of personal health information (i.e., patient data).

1. **We recommend that eHealth Saskatchewan assess risks of inappropriate access to lab results in the Saskatchewan Lab Results Repository and set up related alerts to enable timely detection.**

Addressing security risks includes assessing whether systems are vulnerable to attackers. Systems must be properly configured and regularly updated with security patches to protect them from security vulnerabilities.

eHealth had not properly configured or updated its SLRR systems in a timely manner. For example, we found that eHealth had not applied updates that were available since October 2012 to its SLRR systems. eHealth did not have a documented risk analysis to explain why it did not apply these updates to its SLRR systems. Without proper configuration and timely updates, there is an increased risk someone could gain unauthorized access to systems and data.

2. **We recommend that eHealth Saskatchewan properly configure and update, on a timely basis, its Saskatchewan Lab Results Repository systems for critical vulnerabilities.**

## 5.2 Access Controls Need Strengthening

*We expected eHealth to:*

- *Place physical servers in secured server rooms that are protected against environmental factors (e.g., fire, floods, and temperature extremes), have backup power sources for servers in the event of an electrical outage, and restrict employee access (e.g., by using key cards to access locked rooms and video surveillance to monitor the room)*

- *Have user access controls to control who can access a system (users), the data they can access within that system, and how*

eHealth had contracted a service provider to house, but not manage, its systems and data (i.e., servers) in a data centre. The service provider's data centre had security controls that restrict physical access, supply backup power, and provide environmental controls (e.g., air conditioning).

eHealth had processes for granting and removing user access to the eHR Viewer. User access requests (e.g., new hires and terminations) are processed by eHealth and electronically approved by authorized persons in approved healthcare organizations. We found eHealth maintained appropriate listings of approved healthcare organizations (e.g., RHAs, physicians) and authorized persons within those organizations. We also found eHealth had an appropriate password policy designed to protect the eHR Viewer user accounts from unauthorized access.

However, we found that eHealth did not always remove users in a timely manner (i.e., remove access within one working day of receipt of a termination request). For example,

in one instance, eHealth did not remove access for six working days after its receipt of the request. eHealth's policy does not set a timeframe for implementing changes to user access (e.g., process request within one working day of receipt).

Delays in removing unneeded access mean staff no longer employed by authorized healthcare organizations or who no longer have a need to access patient data continue to have such access.

**3. We recommend that eHealth Saskatchewan implement a policy to require prompt removal of user access to the Saskatchewan Lab Results Repository through the eHR Viewer upon request.**

The confidentiality of SLRR data depends on both eHealth and healthcare organizations sufficiently protecting the system from unauthorized access. While strong processes for making changes to access are critical, a regular review of existing users to verify the continued appropriateness of their access is needed. We found eHealth's policy does not require each approved healthcare organization to confirm, periodically, that its eHR Viewer users continue to have appropriate access. Also, eHealth does not provide these organizations with reports that would help them to efficiently and periodically carry out this review.

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.

**4. We recommend 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.**

eHealth's password policy requires passwords to be changed at least every 90 days. By setting passwords to automatically expire, eHealth forces users to change their password within the required time period. We found eHealth did not set two key accounts with privileged SLRR access (i.e., access with the ability to change systems or data) to expire and the passwords had not been changed in over 90 days. Not changing passwords on a regular basis increases the risk that the password may be compromised.

**5. We recommend that eHealth Saskatchewan follow its password expiry policy for privileged user accounts that access the Saskatchewan Lab Results Repository.**

## 5.3 SLRR May Not be Available in the Event of a Disaster

*We expected eHealth to:*

- *Have effective backup and recovery procedures designed to reduce the amount of downtime for SLRR. This includes storing backed up data on encrypted tapes (i.e., tapes that are unreadable without a code) at an offsite location.*
- *Have a recovery plan for SLRR in the event of a disaster (disaster recovery plan).*

eHealth had effective backup policies and procedures, including storage of encrypted backups at an offsite location. We found that eHealth regularly performed backups of server data and verified daily whether server backups were successful.

eHealth did not have a complete, documented disaster recovery plan in case of a major system failure (e.g., SLRR equipment and data becomes unavailable). eHealth also hosts lab information systems on behalf of RHAs at the same data centre as SLRR, except for the Regina-Qu'Appelle and Saskatoon RHAs. Therefore, a disaster at the data centre would impact SLRR and most RHA lab information systems that are data sources for SLRR. Such a disaster could delay when lab results are available to healthcare providers and impact patient care.

Without a complete and tested disaster recovery plan, SLRR may not be available when needed and, as a result, healthcare providers may not have lab results provided to them on a timely basis. We reported the need for eHealth to have a complete and tested disaster recovery plan in our *2014 Report – Volume 2*, Chapter 7.

## 5.4 System and Data Integrity Maintained

*We expected eHealth to:*

- *Have operational processes for maintaining the data integrity of the SLRR system and monitoring of SLRR to ensure it is operating as planned*
- *Implement change management processes. Processes would include approving and testing system changes before their implementation*

Data compiled in SLRR comes from various RHA lab information systems. To compile lab results in SLRR, eHealth converted lab results to a standard set of data requirements. eHealth had detailed procedures for addressing errors related to data compilation failures.

We found eHealth checked for compilation errors throughout the day. SLRR compiled about 1.5 million lab results each month, generating about 100-200 related compilation errors. During our review of errors, we found eHealth rectified the errors by having RHAs correct and resend the data, or by updating SLRR to allow data to be compiled.

Also, we found that eHealth had documented adequate change management processes. For the changes we reviewed, we found eHealth had appropriately approved and tested the changes, and had documented plans in case the changes failed.

## 6.0 Glossary

**Change Management**—An organized approach for introducing changes into a program or process, used to minimize unintended consequences.

**Configure**—To set up or arrange in order to achieve a specific purpose (e.g., maximize security).

**Data Centre**—A central location for computer network hardware and software, especially storage devices for data.

**Disaster Recovery Plan**—A plan for an organization to restore necessary IT services in the event of an emergency or disaster. A disaster recovery plan is one part of a larger, organization-wide business continuity plan.

**Mask**—A process to prevent patient data in the provincial electronic health record from being viewed by users except as approved by the patient or in special circumstances (e.g., in life-threatening situations where the patient is unable to give approval).

**Network**—A group of computers that communicate with each other.

**Patch**—An update to a computer program or system designed to fix a known problem or vulnerability.

**Physical Access Controls**—The controls in place at an organization that restrict unauthorized people from gaining physical access to computers or network equipment. Examples include locked doors and cabinets, and video surveillance systems.

**Server**—A computer that hosts systems or data for use by other computers on a network.

**User Access Controls**—The controls in place at an organization to restrict use of systems or data to those who have been authorized. These include physical controls such as locked doors or cabinets, as well as computer and network controls such as establishing accounts with specific access rights, requiring passwords, etc.

## 7.0 Selected References

Auditor General of British Columbia. (2010). *The PARIS System for Community Care Services, 2009/2010: Report 7*. Victoria: Author. www.bcauditor.com/pubs/2010/report7/paris-system-community-care-services-access-and-security (20 October 2014).

Auditor General of Canada. (2009). *Electronic Health Records, 2009 Fall Report*. Ottawa: Author. www.oag-bvg.gc.ca/internet/English/parl_oag_200911_04_e_33205.html (20 October 2014).

Chartered Professional Accountants of Canada (CPA) and the American Institute of Certified Public Accountants (AICPA). (2014). *Trust Services Principles, Criteria, and Illustrations*. Toronto: Author.

International Organization for Standardization. (2013). ISO/IEC 27002:2013(E). *Information Technology – Code of Practice for Information Security Management; 2nd Edition*. Geneva: Author.

Provincial Auditor of Saskatchewan. (2014). *2014 Report – Volume 1, Chapter 7, Central Services – Information Technology Division – Data Centre*. Regina: Author.

Provincial Auditor of Saskatchewan. (2014). *2014 Report – Volume 1, Chapter 8, Public Service Commission – MIDAS HR/Payroll*. Regina: Author.

Provincial Auditor of Saskatchewan. (2014). *2014 Report – Volume 1, Chapter 9, eHealth Saskatchewan – Provincial Electronic Health Records*. Regina: Author.

Western Australian Auditor General. (2014). *Information Systems Audit Report, Report 14*. Perth: Author. www.audit.wa.gov.au/wp-content/uploads/2014/06/report2014_14-ISAudit.pdf (23 July 2014).