Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 176-2015

Saskatoon Regional Health Authority

January 29, 2016

Summary: Saskatoon Regional Health Authority (SRHA) proactively reported a privacy breach to the Office of the Information and Privacy Commissioner (OIPC). Following its investigation, SRHA determined that there were broader issues that needed to be addressed by the region including the practice of technologists working in the Department of Medical Imaging sharing user access to the Radiology Information System (RIS) and the Picture Archiving and Communications System (PACS). As a result of these broader issues, the Commissioner found that SRHA was not in compliance with section 16 or subsections 23(1) or (2) of *The Health Information Act* (HIPA). Further, that SRHA's safeguards were not sufficient to protect personal health information. The Commissioner recommended that SRHA strive for an urgent solution to the issue of technologists sharing user access. In addition, he recommended that SRHA implement a manual audit schedule for PACS, finalize its broader audit policy and procedure for all electronic health record systems and ensure that all *User Agreements for RIS/PACS* are signed by employees and physicians. Finally, the Commissioner recommended that the remaining 12 health regions in the province investigate to see if the issues highlighted in the report impact their region and advise his office.

I BACKGROUND

[1] On September 10, 2015, Saskatoon Regional Health Authority (SRHA) contacted my office to proactively report a privacy breach. According to SRHA, one of its technologists had inappropriately accessed personal health information of family members on the Radiology Information System (RIS) and the Picture Archiving and Communications System (PACS). The access was for personal reasons and was not in compliance with *The Health Information Protection Act* (HIPA). SRHA advised that it

had completed its investigation and would provide my office with a copy of its internal investigation report. The report was received on September 17, 2015.

[2] After reviewing SRHA's internal investigation report, I was satisfied with how SRHA addressed the privacy breach. However, broader issues were identified which this Investigation Report will address. Of primary concern, technologists are sharing user access in RIS and PACS in certain situations.

II DISCUSSION OF THE ISSUES

[3] SRHA is a "trustee" pursuant to subsection 2(t)(ii) of HIPA. As a trustee, SRHA is subject to the rules outlined in HIPA as it pertains to the protection of personal health information.

1. Is there personal health information involved in this matter?

[4] Our customary analysis when dealing with a privacy matter under HIPA is to first determine whether there is "personal health information" involved. Subsection 2(m) of HIPA defines "personal health information" as follows:

> **2** In this Act:
>
> …
>
> (m) "**personal health information**" means, with respect to an individual, whether living or deceased:
>
> (i) information with respect to the physical or mental health of the individual;
>
> (ii) information with respect to any health service provided to the individual;
>
> (iii) information with respect to the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;
>
> (iv) information that is collected:
>
> (A) in the course of providing health services to the individual; or

(B) incidentally to the provision of health services to the individual; or

(v) registration information;

[5] In this circumstance, the broader issues that were identified deal with access to personal health information contained in RIS and PACS.

[6] RIS is a computer system for tracking patients and medical imaging procedures including examination scheduling, result reporting and billing. It captures patient demographics and the orders used to schedule and complete an exam. Once an exam is completed, a radiologist will interpret the images and record the results in RIS.

[7] PACS is designed for the storage, retrieval and display of diagnostic images including x-rays, computerized tomography (CT), ultrasounds, magnetic resonance imaging (MRI), positron emission tomography (PET), nuclear medicine and bone densitometry. RIS interfaces with PACS to link images and the interpreted results making both available to the authorized user (eHealth Saskatchewan *Annual Report 2010-2011*).

[8] PACS is used throughout the region by thousands of clinicians to look up patient images. RIS is only used in SRHA’s Department of Medical Imaging by approximately 350 employees. The Department of Medical Imaging consists of Radiologists, resident doctors in training to become radiologists, Medical Radiation Technologists, Ultrasound Technologists, MRI Technologists, Nuclear Medicine Technologists, Nurses and support staff.

[9] PACS Scan is software that is integrated into the PACS application and allows for the uploading of paper documents, such as requisitions, into PACS. This is done through the use of an attached scanner. PACS Scan is only used by technologists in the Department of Medical Imaging that are actively processing images and associated documents. This includes Medical Radiation Technologists, Ultrasound Technologists, MRI Technologists and Nuclear Medicine Technologists. This is approximately 200 of the 350 employees in

SRHA using RIS. I am considering, in this Investigation Report, the issue of sharing user access by only those technologists that utilize PACS Scan.

[10] Based on the type of information involved, it is clear that there would be personal health information of patients involved pursuant to subsections 2(m)(i), (ii), (iv) and (v). Therefore, SRHA is required to protect that personal health information in accordance with HIPA.

2. Is SRHA sufficiently safeguarding personal health information in its custody and/or control?

[11] The duty to protect personal health information is provided for in Parts III and IV of HIPA. Section 16 of HIPA requires SRHA to have adequate written policies and procedures to maintain administrative, technical and physical safeguards. These safeguards must protect against any reasonably anticipated threat or hazard to the security or integrity of the information; and the loss of, unauthorized access to, use or disclosure of the information. Section 16 provides as follows:

> **16** Subject to the regulations, a trustee that has custody or control of personal health information must establish policies and procedures to maintain administrative, technical and physical safeguards that will:
> (a) protect the integrity, accuracy and confidentiality of the information;
> (b) protect against any reasonably anticipated:
> (i) threat or hazard to the security or integrity of the information;
> (ii) loss of the information; or
> (iii) unauthorized access to or use, disclosure or modification of the information; and
> (c) otherwise ensure compliance with this Act by its employees.

[12] Subsections 23(1) and (2) of HIPA provide as follows:

> **23**(1) A trustee shall collect, use or disclose only the personal health information that is reasonably necessary for the purpose for which it is being collected, used or disclosed.
>
> (2) A trustee must establish policies and procedures to restrict access by the trustee's employees to an individual's personal health information that is not required by the

> employee to carry out the purpose for which the information was collected or to carry out a purpose authorized pursuant to this Act.
> …

[13] Subsection 23(1) of HIPA requires that SRHA abide by two principles known as data minimization and need-to-know. *Data minimization* means that SRHA should always collect, use and/or disclose the least amount of personal health information necessary for the purpose. *Need-to-know* means that personal health information should only be available to those employees in an organization that have a legitimate need to know that information for the purpose of delivering their mandated services.

[14] Subsection 23(2) of HIPA requires that SRHA have policies and procedures in place to specifically restrict access to personal health information. Restricting access is another way of protecting personal health information from misuse.

[15] In *Putting it into Practice: Privacy and Security for Healthcare Providers Implementing Electronic Medical Records*, the Canadian Health Informatics Association (COACH) highlighted that the primary objectives of privacy policies were to:

- Prevent and detect malicious activities from occurring;
- Assist in understanding potential security exposures and risks;
- Educating, communicating and promoting security responsibilities to all stakeholders;
- Complying with legislative, privacy and contractual requirements; and
- Identifying consequences of security policy violations.
  (2013, at p. 9)

[16] SRHA does have a suite of policies. In particular, its *Privacy and Confidentiality Policy #7311-75-003* which extensively lays out an employee's obligations around protecting personal health information. In addition, SRHA has two agreements that are signed by employees which are relevant in this matter; the *User Agreement for RIS/PACS* and the *Saskatoon Health Region Confidentiality Agreement.*

[17] SRHA has a number of policies and procedures. A significant issue in this case, is the policy, procedure and agreements do not reflect what is being practiced by employees on the front lines. The following three issues will be addressed in this Investigation Report:

i. Technologists are not logging off between sessions in RIS and PACS;
ii. Regular proactive auditing of PACS is not occurring; and
iii. The *User Agreement for RIS/PACS* was outdated.

i. Technologists are not logging off between sessions in RIS and PACS

[18] In its investigation, SRHA determined that technologists were working under each other's log-ins in RIS and PACS. In other words, one technologist would log in and that technologist, along with others on the unit would complete their work under RIS and PACS under one log-in.

[19] I am advised that what is leading to technologists sharing user access on RIS and PACS is the following:

- Only one person can run PACS Scan at one time for any given workstation so each technologist would need to log-off from RIS and PACS between patients in order for other technologists to use PACS Scan; but

- It is too time-consuming to log-in and out of RIS and PACS between patients.

[20] In practice, the problem would look like this:

- A technologist finishes with a patient, logs-in to the workstation computer, logs-in to RIS and PACS, scans the necessary documents via PACS Scan, locks the workstation computer under his/her log-in and leaves;

- The next technologist finishes with a patient, logs into the workstation computer, logs-in to RIS and PACS and attempts to scan documents via PACS Scan but cannot because a pop-up shows up indicating that only one instance of PACS Scan can be running at one time.

[21] If a technologist logged off from all applications between patients, I am advised that it would take three to five minutes to log back in depending on the speed of the computer and the network on the given day in question. The log-in steps include:

- Log-in to the computer workstation using username and password;

- Launch and log-in to the PACS application using username and password;
  - Once logged in, navigate to the current work-list and select the area the technologist is working in;

- Launch and log-in to the RIS application (this requires two sets of usernames and passwords to launch);
  - Once logged in, navigate to technologist worklist screen and select the area the technologist is working in.

[22] On November 25, 2015, staff of my office attended the Royal University Hospital in Saskatoon. They learned that in the area of general x-ray, there were typically three to four technologists using two to three computer workstations positioned outside of two exam rooms. On a busy day, the technologists process a new examination every two to four minutes. During peak times, more technologists are sharing the computer workstations so multiple technologists need access to a limited number of workstations. To log-in and out between patients would slow the delivery of service to a snail's pace. The technologists solved the inefficiency by logging in to all applications (computer, RIS and PACS) and leaving the workstation open so they could each go back and forth between patients to complete their work quickly using the scanner. Although efficient, the solution is not in line with HIPA, SRHA's *Privacy and Confidentiality Policy #7311-75-003* or the *Saskatoon Health Region Confidentiality Agreement* signed by employees at the time of hire.

[23] In order to solve this problem, it appears there are two options:

- Either increase the number of technologists that can run PACS Scan at one time; and/or

- Simplify the log-in process for RIS and PACS so technologists can log-in and out between patients quickly.

[24] SRHA has advised that it is exploring a number of solutions including:

- Providing all users with their own workstations;
- Going paperless;
- Designating a medical office assistant to do all the scanning; or
- Finding a technological solution.

[25] SRHA has advised my office that each of the potential solutions has inherent challenges. Providing all users with their own workstations would be extremely expensive and the funding is not available in the region at this time. There is also limited physical space to accommodate the number of workstations that would be needed. There are approximately 200 technologists in the region impacted by this issue.

[26] According to SRHA, going paperless is not currently an option as physicians are still heavily reliant on paper requisitions and communications which require scanning. Even if the region went paperless, it would be receiving paper that it would have to deal with. In the future, a fully electronic health record may solve this issue.

[27] SRHA explored having a medical office assistant do all of the scanning. However, SRHA indicated that this could compromise patient safety due to the potential risk of linking scanned information to the wrong patient. Presently, technologists do this at the point of patient contact.

[28] Also, a number of technological solutions are being explored. SRHA plans to discuss options with the three vendors involved with RIS, PACS and PACS Scan to see if a solution is available that will either allow multiple users to run PACS Scan at one time or enable a quicker log-in for RIS and PACS. I am advised that at the present time, none of the vendors have offered a solution that will work.

[29] A proof of concept of tap and go technology is currently being planned in the Department of Medical Imaging. If the proof of concept appears to be a potential solution, a pilot would likely be started in one location. Tap and go is technology that enables a user to tap a card to log-in and tap again to log-out. It is too early to know if this technology would work. There are concerns that it may not be able to get around the numerous log-in steps involved with RIS.

[30] Until a solution is found, SRHA is allowing technologists to continue the practice of working under each other's log-ins. Unfortunately, this ongoing practice leaves SRHA not in compliance with section 16 and subsections 23(1) and (2) of HIPA.

[31] I recommend that SRHA strive for an urgent solution and provide my office with quarterly updates of its progress.

[32] During this investigation, it came to my attention that other health regions in the province were likely dealing with the same issue of technologists not logging off between sessions in RIS and PACS. If this is the case, these regions would also not be in compliance with section 16 and subsections 23(1) and (2) of HIPA. It is expected that all remaining 12 health regions in the province investigate to see if this issue impacts their region and advise my office of its plans to address it.

ii. Regular auditing of PACS was not occurring

[33] When an allegation of a privacy breach involving inappropriate access to an electronic health record system is reported, SRHA will run an audit in the system to determine if inappropriate access had occurred. However, during its investigation of this privacy breach, SRHA discovered that it was difficult to audit the technologist's accesses in PACS due to the practice of technologists working under each other's log-ins. In addition, it discovered that PACS was not being routinely audited.

[34] Auditing is a technical safeguard. It is a manual or systematic measurable technical assessment of employee access to a system or application. Auditing of information systems is necessary to:

- Assess compliance with and measure effectiveness of policies and procedures;
- Assess compliance with legislative requirements;
- Assess whether appropriate measures are in place to control access; and
- Monitor access.

[35] In *Putting it into Practice: Privacy and Security for Healthcare Providers Implementing Electronic Medical Records*, COACH outlines guidelines and best practices including the need for an audit program. An audit program includes regular monitoring of behavior to determine whether users are complying with the organizations privacy and security policies when accessing and using data. Further, it serves as a deterrent to unauthorized access to patient records, and it supports other privacy activities, including providing evidence for the investigation of privacy breaches and privacy complaints. Monitoring for compliance with policies and procedures can identify gaps in user training and awareness, and areas that need reinforcement. It can also provide information useful for modifying a role-based access control model. An audit program is one component of a comprehensive risk management program (2013, at p. 41).

[36] SRHA's *Privacy and Confidentiality Policy #7311-75-003* states that the region audits electronic health record systems. The policy states:

> **3.3.2** SHR audits EHR applications for compliance with this policy.

[37] One policy and procedure that SRHA does not have in place is a broader audit policy for its electronic health record systems. I am advised that this policy has been worked on and is in draft form. There is no indication from SRHA as to when it will be finalized or implemented. By not having this policy and procedure in place, the health region is not in compliance with section 16 and subsection 23(2) of HIPA.

[38] The practice of technologists working under each other's log-ins challenges SRHA's ability to authenticate authorized users. However, a well-established audit program,

which includes a policy and procedure would enable SRHA to at least reduce the risk of inappropriate access given this practice will continue for some time.

[39] It is acknowledged that the practice of sharing user access makes it difficult for SRHA to effectively audit because it is unclear which technologist accessed information in PACS and from which workstation. For this reason, the typical automated audit would not work. However, SRHA has indicated that it can manually audit accesses to look for inconsistencies such as the location of an employee, the location of a patient, who is on shift, or same name look-ups (i.e. employees accessing patients with the same last name, such as family members). This is more time consuming. Therefore, SRHA indicated that it could manage a manual audit of two days of information in PACS audited randomly once per month.

[40] I requested an update from SRHA on the status of its manual audits of PACS. SRHA indicated that it was overdue but would be implementing a regular schedule in January 2016. SRHA advised that previous audits done last summer did not show anything out of the ordinary.

[41] If SRHA is allowing technologists to work under each other's log-ins until a solution can be found, it is critical that SRHA at least mitigate the risk of inappropriate access to personal health information in PACS through the use of regularly scheduled random audits. In addition, employees should be advised that this is occurring. This should act as a strong deterrent.

[42] Therefore, I recommend that SRHA implement the manual audit schedule of two days of information in PACS audited randomly once per month beginning in February 2016.

[43] In addition, I recommend that SRHA finalize its broader audit policy and procedure for all electronic health record systems by July 1, 2016 and have it implemented by October 1, 2016.

iii. The User Agreement for RIS/PACS was outdated

[44] When an employee in the Department of Medical Imaging is granted user access to RIS and PACS, they sign a user agreement. SRHA determined during its investigation that the Department of Medical Imaging had been using an outdated agreement. The agreement was deficient in a number of respects; most importantly it lacked language around the sharing of usernames and passwords and on accessing RIS and PACS only when necessary to perform assigned duties on a need-to-know basis and in compliance with HIPA.

[45] SRHA revised its *User Agreement for RIS/PACS* to state that users should not share their PACS and/or RIS username and/or password with anyone. In addition, employees were not to use their position in SRHA to collect, access or disclose personal health information that was not required for employment-related purposes.

[46] However, SRHA had difficulty getting all employees and physicians with access to RIS and PACS within the region to sign the new agreement. Resistance to sign seemed focused on the language used in the new agreement specifically around accessing the system for employment-related purposes. For example, a physician who conducts research and has access to PACS responded to the request to sign the new agreement with the following email:

> The following text is unacceptable:
>
> > "I understand and acknowledge that I shall not use my position in [SRHA] in order to collect or access or disclose personal health information that is not required for employment-related purposes."
>
> In specific, the manager of radiology is in no position to ascertain if my use of personal health information is legitimate or not. He has no research role and is not part of the [location of researcher] structure, which would be a main reason for accessing data. You have to decide when something is none of your business. Fix this to include legitimate uses not under your direct supervision. And QA for professionals, and research in [sic] not in your purview. If you want, I can change it for you, since you seem not able to react in a timely fashion to complaints about your own ability to react to reasonable requests. You make your linguistic paralysis my problem. I have news for you, it is your problem not mine.

[47] This response speaks to the challenges faced by the SRHA privacy team, the Department of Medical Imaging and SRHA as a whole. SRHA has also been dealing with legal counsel representing certain professions within the region who are resistant to sign the agreement due to wording of certain clauses. The current version of the new agreement has been changed again to state that users should only access PACS and RIS when necessary to perform their duties on a need-to-know basis or in compliance with HIPA.

[48] I requested an update from SRHA on whether all relevant employees and physicians had, at this point, signed the updated *User Agreement for RIS/PACS*. SRHA advised that there were hundreds of employees required to sign the agreement as PACS was a widely utilized system. This included more than just the technologists affected by the issue of log-ins. At the time of this Investigation Report, it had agreements signed by 931 employees. Over the coming weeks, SRHA intends to compile a list of users that had not signed the new agreement and follow-up with these users accordingly.

[49] A signed user agreement is where employees acknowledge their privacy and security responsibilities for protecting the confidentiality of personal health information they are being given access to. SRHA's *Privacy and Confidentiality Policy #7311-75-003* states the following:

> **3.3.1** Staff may also be required to sign Confidentiality Acknowledgement(s) specific to Electronic Health Record (EHR) applications.

[50] In *Privacy in Saskatchewan Health Care: An Overview*, the College of Physicians and Surgeons of Saskatchewan highlighted the importance of patient confidence:

> Privacy is a major concern for physicians. The increased availability of patient records in electronic format has led to concerns about the potential misuse of personal information for purposes other than direct patient care. Without confidence that their privacy will be maintained, patients may refrain from disclosing critical information, may refuse to provide their consent to use personal health information for research purposes, or may simply not seek treatment.

[51] I recommend that SRHA ensure that the *User Agreement for RIS/PACS* is signed by the remaining employees and physicians by October 1, 2016. Further, for any remaining employees and physicians that have not signed the new agreement by this date, SRHA suspend their user access privileges for RIS and PACS until it is signed.

[52] In conclusion, given all of the issues outlined here, I find that SRHA is not able to restrict access to personal health information in RIS and PACS to only those employees that have a need-to-know as required by subsections 23(1) and (2) of HIPA. This means it cannot protect personal health information from the threats contemplated at section 16. Therefore, I find that SRHA's safeguards are not sufficient.

[53] On January 26, 2016, my office provided SRHA with its preliminary findings and recommendations as outlined below. On January 28, 2016, SRHA responded indicating that it wanted its patients to trust that it had taken every step to ensure that their health information was protected. It agreed to comply with all of my office's recommendations.

[54] In this Investigation Report, I have determined that other health regions in the province may be dealing with the same issues. Therefore, at the end of this Investigation Report a broader recommendation has been made to all remaining 12 health regions in the province. My office will send this Investigation Report to the health regions requesting that they investigate and provide a written response to my office by February 29, 2016. My office will follow up accordingly on these responses.

III FINDINGS

[55] I find that SRHA is not in compliance with section 16 or subsections 23(1) and (2) of HIPA.

[56] I find that SRHA's safeguards are not sufficient to protect personal health information.

IV RECOMMENDATIONS

a. Saskatoon Regional Health Authority

[57] I recommend that SRHA strive for an urgent solution to the issue of log-ins and provide my office with quarterly updates of its progress.

[58] I recommend SRHA implement the manual audit schedule of two days of information in PACS audited randomly once per month beginning in February 2016.

[59] I recommend that SRHA finalize its broader audit policy and procedure for all electronic health record systems by July 1, 2016 and have it implemented by October 1, 2016.

[60] I recommend that SRHA ensure that all *User Agreements for RIS/PACS* be signed by employees and physicians in the region by October 1, 2016. Further, for any remaining employees and physicians that have not signed the new agreement by this date, I recommend SRHA suspend their user access privileges for RIS and PACS until it is signed.

b. Other health regions in Saskatchewan

[61] I recommend that the remaining 12 health regions in the province investigate to see if the issues highlighted in this Investigation Report impact their region and advise my office of its plans to address them by February 29, 2016. This includes:

1. Cypress Health Region
2. Keewatin Yatthe Health Region
3. Prairie North Health Region
4. Athabasca Health Region
5. Five Hills Health Region
6. Kelsey Trail Health Region
7. Prince Albert Parkland Health Region
8. Sun Country Health Region

9. Heartland Health Region
10. Mamawetan Churchill River Health Region
11. Regina Qu'Appelle Health Region
12. Sunrise Health Region

Dated at Regina, in the Province of Saskatchewan, this 29th day of January, 2016.

Ronald J. Kruzeniski, Q.C.
Saskatchewan Information and Privacy
Commissioner