Office of the
Saskatchewan Information
and Privacy Commissioner

# INVESTIGATION REPORT 164-2023, 226-2023, 227-2023, 228-2023, 229-2023, 268-2023, 274-2023, 275-2023, 277-2023, 278-2023, 279-2023, 280-2023, 299-2023, 308-2023

**Saskatchewan Health Authority, Saskatchewan Cancer Agency, Ministry of Health, Prince Albert Co-operative Health Centre, City Centre Family Physicians (Stonebridge Holdings Inc.), Kenderdine Medical Clinic (Dr. Marlys Misfeldt, Dr. Aimo Berger, Dr. Bisayo Olabiyi, Dr. Olanrewaju Olabiyi, Dr. Glen Daguio, Dr. Stefan Van Niekerk, Carinca Leroux Van Niekerk, Dr. Oluyemisi Ojelabi), South Hill Medical Practice (Dr. L.N. De Beer Medical Professional Corporation, 101139574 Saskatchewan Ltd.), Wall Street Obstetrics and Gynaecology (Dr. Paige Grenier Medical Prof. Corp., Dr. Vanessa Rininsland Medical Prof. Corp., Drs. M. Ng and R. Rajakumar Medical P.C. Inc.), Dr. Dalisizwe Dewa, Willowgrove Medical Group (Surgimed Medical Professional Corporation, Dr. Colin Halbgewachs Medical Prof. Corp., Adegboyega Ketiku M.D., Professional Corporation, Dr. Moses Olakanmi Medical Prof. Corp.), Herold Road Family Physicians (Dr. Myles Deutscher, Dr. Paula Schwann, Dr. Aaron Friggstad, Dr. Andrea L. Symon, Dr. Andrea Jill Davis, Dr. Marketa Chaloupka, Dr. David Woloschuk, Dr. Robyn Lynn Tenaski), Dr. Colin Pearce**

**January 17, 2024**

**Summary**: Dr. D. Marciniuk reported that they received multiple misdirected faxes and mail that were intended for other physicians with the same last name. The Commissioner initiated 14 investigations into the incidents. After investigating the matters, the Commissioner found that the trustees involved had disclosed personal health information without authority. The Commissioner found that the privacy breaches were contained, and in some cases the affected parties were notified. In all cases, he found that the notices were not sent within a reasonable time. The Commissioner found that SHA's notice to the affected parties was not adequate in that it did not advise parties of their right to file a complaint with his office. The Commissioner also found that all trustees completed investigations, but they failed to

identify all of the measures that should be taken to prevent further breaches of this kind in the future. The Commissioner recommended that SHA take additional actions to address the systemic problem of misdirected faxes including the need to ensure that all individuals with access to personal health information receive annual privacy training. The Commissioner also made specific recommendations on the actions other trustees could take to prevent further breaches of this kind.

## I BACKGROUND

[1] This Investigation Report involves 85 misdirected faxes and one misdirected letter sent by mail that were reported to my office by a physician named Dr. Darcy Marciniuk (Dr. DM) – the recipient of the misdirected communications. In some cases, the faxes were intended for Dr. Jeffrey Marciniuk (Dr. JM). Dr. JM has the same specialty as Dr. DM and both physicians practice medicine in Saskatoon. In one case, a fax should have been sent to Dr. Tanya Marciniuk (Dr. TM) who also practices in Saskatoon. The misdirected letter should have been sent to Dr. JM.

[2] Dr. DM advised my office that they had been receiving misdirected faxes intended for Dr. JM since approximately July 2020. The samples provided to my office date from August 2020 onwards.

[3] It appears that 109 individuals were affected by a total of 86 misdirected communications. The records included echocardiography reports, cardiology reports, hospital discharge records, lung function reports, ophthalmology reports, pathology reports, lab results, medical imaging results, patient care notes, referral letters and consultation notes. Notably, Dr. DM advised that some of the records included information that was critical to patient care.

[4] Dr. DM advised that they routinely redirected the faxes and mail to the intended recipient and advised the sending organization of the error. Despite that, in many of the cases reported to my office, the sending organization continued to send Dr. DM records that were intended for Dr. JM. For example, Dr. DM reported that the Roy Romanow Provincial

Laboratory sent them one misdirected fax in September 2020, one in October 2021, six in May 2023 and one in June 2023. Royal University Hospital Medical Imaging department sent one in December 2020, two in November 2022, and one in May 2023. All of these organizations fall under the Saskatchewan Health Authority (SHA).

[5] Dr. DM tried to address the problem informally by contacting the SHA Privacy Office in February of 2023. However, no one returned his call.

[6] The senders of the faxes included large organizations such as the SHA and the Saskatchewan Cancer Agency (SCA).

[7] Other senders were clinics where multiple health care providers provide health services. Some senders were sole practitioners. In some cases, the physician providing the service was responsible for sending the fax and in other cases administrative staff may have been involved.

[8] The majority of the misdirected faxes involved the use of digital fax machines with built in directories or address books for physicians, pharmacies and others. In some cases, misdirection arose when an individual received unclear direction as to the recipient from a physician. In other cases, the wrong or incomplete name was provided by the patient to the health care provider or registration staff. In some cases, the sender chose the wrong recipient from the directory. In other cases, Dr. JM’s name did not appear in the directory. In all cases, human error contributed in some way to the breaches.

[9] The move away from the traditional fax machine is an important measure to reduce the risks of privacy breaches. My office is a proponent of electronic information management systems. However, the use of these systems does not eliminate the risk of error by the user. To address this risk, clear policies and procedures setting out rules and defining roles, and repeated privacy training and privacy awareness raising activities are essential safeguards. Comprehensive and mandatory annual privacy training is essential to reinforce defined processes and procedures, and the development and maintenance of a culture of privacy.

[10] Since 2018, my office has investigated approximately 70 incidents of misdirected faxes and issued 17 investigation reports involving misdirected faxes under *The Health Information Protection Act* (HIPA). Many of the reports involved multiple misdirected faxes. For example, Investigation Report 045-2021, et al involved 23 misdirected health records originating from four different trustees.

[11] In at least three previous reports issued by my office, misdirected faxes were sent to a physician with a similar name as the intended recipient or clinics with similar sounding names (see for example, Investigation Reports 045-2023, et al, 032-2022 and 126-2021). As trustees do not report all misdirected faxes to my office, I do not know how many more misdirected fax breaches may have occurred in this time.

[12] In previous investigation reports, I have expressed serious concerns about the privacy risks that arise from the ongoing use of traditional faxes to send personal information and personal health information. I have also noted the need for adequate safeguards when personal health information is shared through traditional fax machines and digital faxing systems.

[13] I am particularly concerned about Dr. DM's view regarding the potential impact that misdirected faxes may have on health care services and patients' health.

[14] Other privacy oversight authorities share my concerns. Canada's federal, provincial and territorial privacy commissioners and ombudspersons passed a resolution in September 2022 titled, "Securing Public Trust in Digital Healthcare." The resolution calls for a concerted effort across the healthcare sector to modernize and strengthen privacy protections for sharing personal health information. It urges stakeholders to phase out the use of traditional fax machines. It also urges health sector institutions and providers using digital alternatives to traditional fax machines to design and adopt governance frameworks that provide reasonable safeguards to protect personal health information. My hope is that Saskatchewan's trustees will heed this call to action.

[15] My office notified the trustees responsible for the misdirected communications to Dr. DM that we would be undertaking a privacy breach investigation pursuant to subsection 52(d) of HIPA. The notice requested that the relevant organizations or bodies investigate the matter and provide my office with a completed *Privacy Breach Investigation Questionnaire* (Questionnaire). My office has received completed Questionnaires from all the trustees.

## II DISCUSSION OF THE ISSUES

### 1. Do I have jurisdiction?

[16] HIPA applies when three elements are present: (1) personal health information, (2) a trustee, and (3) the personal health information is in the custody or control of the trustee.

[17] The information contained in the 86 misdirected faxes varied. They included an individual's name and health services number. In some cases, the individual's address, telephone number, birthdate, gender, information about their health, health services received, and their physicians' names were also included. This information qualifies as "personal health information" as defined by subsections 2(1)(m)(i), (ii) and (v) of HIPA.

[18] Subsections 2(1)(m)(i), (ii) and (v) of HIPA provide:

> **2**(1) 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;
>
> …
> (v) registration information;

[19] Next, I will review whether trustees are involved. The relevant provisions of HIPA are as follows:

> **2**(1) In this Act:
>
> ...
> (t) "trustee" means any of the following that have custody or control of personal health information:
>
> ...
> (ii) the provincial health authority or a health care organization;
>
> …
> (xi) the Saskatchewan Cancer Foundation:
>
> …
> (xii) a person, other than an employee of a trustee, who is:
>
> (A) a health professional licensed or registered pursuant to an Act for which the minister is responsible; or
>
> …
>
> (xiv) a person, other than an employee of a trustee, who or body that provides a health service pursuant to an agreement with another trustee;
>
> (xv) any other prescribed person, body or class of persons or bodies;

[20] Regarding subsection 2(1)(t)(xi) of HIPA and the SCA, I note that section 3 of *The Cancer Agency Act* provides:

> **3** The Saskatchewan Cancer Foundation established pursuant to The Cancer Foundation Act, as that Act exited before the coming into force of this Act, is continued as a corporation under the name of the Saskatchewan Cancer Agency.

[21] Subsection 4(b) of *The Health Information Protection Act Regulations* (HIPA Regulations) is also relevant here. It provides:

> **4** For the purposes of subclause 2(1)(t)(xv) of the Act, the following are prescribed as trustees:
>
> …

> (b) every person who owns or operates a privately-owned facility in or from which health services are provided by a health professional;

[22] Section 2-29 of *The Legislation Act* applies to the interpretation of statutes in Saskatchewan. It states that the term "person" as used in an enactment in Saskatchewan includes a corporation.

[23] Dr. Colin Pearce and Dr. Dalisizwe Dewa are trustees pursuant to subsection 2(1)(t)(xii)(A) of HIPA.

[24] SHA manages Saskatoon City Hospital, Roy Romanow Provincial Laboratory, Wadena Hospital, Royal University Hospital, St. Paul's Hospital, Jim Pattison Children's Hospital, Humboldt District Health complex, Rosetown Health Centre, Preeceville Primary Health Care, and Canora Health and Wellness Centre from which the misdirected faxes at issue in investigation files 164-2023 and 229-2023 originated. SHA is a trustee pursuant to subsection 2(1)(t)(ii) of HIPA.

[25] The SCA is a trustee pursuant to subsection 2(1)(t)(xi) of HIPA. The Ministry of Health (Health) is a trustee pursuant to subsection 2(1)(t)(i) of HIPA.

[26] In my office's Investigation Report 239-2017, I found that the Prince Albert Co-operative Health Centre (PACHC) is a trustee pursuant to subsection 2(1)(t)(xiv) of HIPA. That finding was based on an agreement between Health and the PACHC for the provision of health services in which PACHC acknowledged it was a trustee and that HIPA applied. That agreement was extended to March 31, 2024, and therefore, it continues to apply today. Therefore, I find that PACHC is a trustee.

[27] City Centre Family Physicians (CCFP) is solely owned by Stonebridge Holdings Inc., and it is a privately owned facility from which health services are provided by health professionals.

[28] As noted above, the term "person" as used in an enactment in Saskatchewan includes a corporation pursuant to section 2-29 of *The Legislation Act*. Therefore, Stonebridge Holdings Inc. qualifies as a "trustee" under subsection 4(b) of the HIPA Regulations. The owners will be referred to as CCFP throughout this Investigation Report.

[29] Kenderdine Medical Clinic (KMC) is owned by Dr. Marlys Misfeldt, Dr. Aimo Berger, Dr. Bisayo Olabiyi, Dr. Olanrewaju Olabiyi, Dr. Glen Daguio, Dr. Stefan Van Niekerk, Carinca Leroux Van Niekerk and Dr. Oluyemisi Ojelabi. KMC is a privately operated facility offering health services provided by health professionals. Therefore, the owners of KMC qualify as "trustees" pursuant to subsection 4(b) of the HIPA Regulations. The owners will be referred to as KMC.

[30] Wall Street Obstetrics and Gynaecology (WSOG) is owned by Dr. Paige Grenier Medical Prof. Corp., Dr. Vanessa Rininsland Medical Prof. Corp. and Drs. Ng and R. Rajakumar Medical P.C. Inc. As owners of a privately operated facility offering health services by health professionals, they qualify as "trustees" pursuant to subsection 4(b) of the HIPA Regulations. They will be referred to as WSOG.

[31] Willowgrove Medical Group (WMG) is a clinic owned by four persons. They are Surgimed Medical Professional Corporation, Dr. Colin Halbgewachs Medical Prof. Corp., Adegboyega Ketjku M.D. Professional Corporation and Dr. Moses Olakanmi Medical Prof. Corp. They are persons who own a privately operated facility offering health services by health professionals. Therefore, they qualify as "trustees" pursuant to subsection 4(b) of the HIPA Regulations and will be referred to as WMG.

[32] The Herold Road Family Physicians (HRFP) is a clinic owned by eight physicians. They are Dr. Myles Deutscher, Dr. Paula Schwann, Dr. Aaron Friggstad, Dr. Andrea L. Symon, Dr. Andrea Jill Davis, Dr. Marketa Chaloupka, Dr. David Woloschuk and Dr. Robyn Lynn Tenaski. They are owners of a privately operated facility offering health services by health professionals. Therefore, they qualify as "trustees" pursuant to subsection 4(b) of the HIPA Regulations and will be referred to as HRFP.

[33] South Hill Medical Practice (SHMP) is owned by Dr. L.N. De Beer Medical Professional Corporation and 101139574 Saskatchewan Ltd. As owners of a privately operated facility offering health services by health professionals, they qualify as "trustees" pursuant to subsection 4(b) of the HIPA Regulations. They will be referred to as SHMP.

[34] Finally, I must determine if the trustees had custody or control over the personal health information at issue. "Custody" is physical possession with a measure of control.

[35] Since all the faxes originated from the trustees, I find that the trustees have custody over the personal health information. Therefore, the third element is also present.

[36] As all three elements are present, I find that HIPA applies, and I have jurisdiction to investigate these matters.

**2. Did a privacy breach occur?**

[37] A privacy breach occurs when a trustee collects, uses, or discloses personal health information in a way that is not authorized by HIPA.

[38] The term "disclose" means sharing personal health information with a separate entity that is not a division or a branch of the trustee organization.

[39] The trustees disclosed personal health information when they sent the personal health information to the wrong recipient. The trustees acknowledged that the disclosures were not authorized. I find that breaches of privacy occurred in every case.

**3. Did the trustees respond appropriately to the privacy breaches?**

[40] In privacy breach investigations, my office determines whether the trustee appropriately responded to the breach. In accordance with my office's *Rules of Procedure,* my office will consider whether the trustee appropriately:

- Contained the breach (as soon as possible)
- Notified affected individuals (as soon as possible)
- Investigated the breach
- Took appropriate steps to prevent future breaches.

***Contain the breach***

[41] On learning that a privacy breach has occurred, a trustee should immediately take steps to contain it or reduce the risks. My office's *Privacy Breach Guidelines for Trustees* (August 2022), at page 3, states that containment may involve:

- Stopping the unauthorized practice
- Recovering the records
- Shutting down the breached system
- Revoking access to personal health information
- Correcting weaknesses in physical security.

[42] Effective and prompt containment reduces the magnitude of a breach and the risks involved with the inappropriate disclosure of personal health information.

[43] In assessing the steps taken to contain a breach, my office applies a reasonableness standard (see for example, my office's Investigation Report 145-2023, 147-2023).

[44] Dr. DM confirmed that in each of the cases of misdirected communications their office redirected the fax to the appropriate recipient and deleted or destroyed any copies received. They also notified the sender trustees that the communication had been misdirected. This appears to be consistent with the information provided to my office from the trustees responsible for the breaches. I am satisfied that the breaches were appropriately contained.

***Notify affected individuals***

[45] It is important to notify an individual that their personal health information was inappropriately disclosed for several reasons. Not only do individuals have a right to know, but they also need to know to protect themselves from any potential harm that may result from the inappropriate disclosure. Unless there is a compelling reason not to, trustees should always notify affected individuals.

[46] My office's *Privacy Breach Guidelines for Trustees*, at page 4, states that notification should happen as soon as possible after the key facts about the breach have been established. These guidelines also set out what a notification should include:

- A general description of what happened
- A detailed description of the personal health information involved (e.g., name, medical record, etc.)
- A description of the types of harm that may result from the privacy breach
- Steps taken and planned to mitigate the harm and to prevent future breaches
- If necessary, advice on actions the individual can take to further mitigate the risk of harm and protect themselves (e.g., how to change a health services number)
- Contact information of an individual within the organization who can answer questions and provide information
- A notice that individuals have a right to complain to the IPC
- Recognition of the impacts of the breach on affected individuals and an apology.

[47] In some of the cases, the trustees notified the affected individuals, but not in all. The details of the steps taken to notify affected individuals for each investigation file are set out below.

[48] Where notice was provided, the trustees failed to notify the affected parties within a reasonable time frame. This appears to have been because staff who were made aware of the privacy breaches, did not notify a person responsible for privacy in their organization.

It appears that in many cases, physicians and staff did not understand that a privacy breach had occurred.

[49] In Part III of this Investigation Report, I provide a summary of the trustees' efforts to notify affected parties, other than SHA. I now turn to my analysis of SHA notification efforts.

**SHA**

[50] Following is my analysis of SHA's notification efforts in investigation files 164-2023 and 229-2023.

[51] It appears that as of the date of this Investigation Report, the SHA has not notified all affected parties. I recommend that SHA complete its notifications of affected parties within 30 days of issuance of this Investigation Report.

[52] Where SHA did notify affected parties, the notice was not sent until after my office sent its Notice of Investigation to SHA. The notices were not sent as soon as possible after learning of the breaches because staff involved either were not aware that a breach had occurred or did not follow policy that requires that the SHA privacy office be notified of a breach. I will return to this subject later in the context of a discussion about the important safeguard of training and awareness.

[53] I was provided with a sample or template for the notice that was sent to the affected parties. I note that the template does not include a statement about the affected parties right to file a complaint with my office. Nor does it include any contact details for my office. I find that the notices to affected parties did not comply with the best practices set out in paragraph [46] of this Investigation Report.

[54] I note that in my office's Investigation Report 145-2023, 147-2023, I recommended that SHA ensure that its notification letters to affected individuals include their right to

complain to my office and contact information for my office. It appears that SHA accepted this recommendation, but it has not taken any action to address it.

[55] SHA provided my office with a copy of its draft work standard "Notifying an individual affected by a privacy breach." Appendix B to the work standard sets out a checklist for what should be included in the notice. It does not refer to a requirement to include information about the right to file a complaint with my office. I recommend that SHA revise the draft work standard within 30 days of issuance of this Investigation Report to require that notices include a statement about the right to complain to my office.

[56] SHA advised my office that in the 2022-2023 fiscal year, the privacy office received notice of 37 incidents of misdirected communications which included fax, mail and email. In the 2023-2024 fiscal year (to January 4, 2023), SHA's privacy office received notice of 92 misdirected communications. It advised that it was not able to provide my office with the statistics for prior to March 31, 2022. I note that these numbers would not include the misdirected communications that were not reported to the privacy office, such as those at issue here.

[57] Due to the volume of incidents of misdirected faxes from within SHA, in previous reports, I have recommended that SHA proactively report all misdirected fax breaches to my office (see for example Investigation Reports 120-2022, 135-2022, 045-2021, et. al., 032-2022, 080-2022 and 081-2022). This would enable my office to track and report publicly on the progress of SHA's efforts to address the privacy risks and bring some transparency and accountability to its work to address this problem. SHA has stated that it does not agree with this recommendation. In response to Investigation Report 120-2022, 135-2022, it stated:

> The SHA does not agree with this recommendation. Patients are notified of misdirected faxes, and in most cases, they are satisfied with the response of the SHA. Patients are always informed of their right to contact your office should they be dissatisfied. We proactively report misdirected faxes where the volume of patient information is high or the types of personal health information involved is particularly sensitive.

[58] I accept that some individual patients may be satisfied with SHA's response to a misdirected fax. These patients may not be aware of the magnitude of the problem and the potential risks. In addition, affected parties who are not aware of the right to complain to our office from the outset, may not contact the SHA. In those cases, SHA would have no knowledge of whether they are satisfied. I continue to believe that the public interest is best served by SHA notifying my office of all breaches involving misdirected faxes. I will repeat my recommendation that SHA proactively report all misdirected fax breaches to my office.

***Investigate the breach***

[59] Once the breach has been contained and appropriate notification has occurred, the trustee should continue its internal investigation. At the conclusion of its investigation, the trustee should understand the cause of the breach. This will inform how to prevent future breaches.

[60] As noted in the *Privacy Breach Guidelines for Trustees*, at page 5, investigating the privacy breach to identify the root cause(s) is key to understanding what happened and preventing similar privacy breaches in the future. Below are some key questions to ask during a privacy breach investigation:

- When and how did your organization learn of the privacy breach?
- What occurred?
- How did the privacy breach occur?
- What is the applicable legislation and what specific sections are engaged?
- What safeguards, policies, and procedures were in place at the time of the privacy breach?
- Was the duty to protect met?
- Who are the affected individuals?

[61] In Part III of this Investigation Report, I provide a summary of the investigations carried out by the trustees, other than SHA, and the root causes that the investigations identified. I now turn to my analysis of SHA's efforts to investigate the breaches.

**SHA**

[62] With respect to investigation file 164-2023 which involved the SHA, the privacy office stated that it first learned of the privacy breaches when contacted by my office on September 29, 2023. The privacy office contacted the managers in the relevant departments who were asked to investigate. The privacy breaches occurred within multiple different hospitals and departments and impacted 73 individuals. Of the 73 breaches, seven involved traditional fax machines.

[63] SHA stated that the sending department should have contacted the privacy office to report the breaches and noted that additional education is required so that staff know what to do when there is a breach.

[64] It added that the breaches were not intentional and resulted from a failure to follow proper procedures. It also stated that the breaches were caused by "weakness of administrative safeguards." When asked to provide further information about the safeguards that were considered weak, SHA pointed to human error and heavy workload.

[65] Regarding the root cause, I will reproduce what information was provided to my office by the SHA. It stated:

> There were multiple reasons that contributed to the breach:
>
> - Registration entered incorrect attending physician, ordering provider auto-fills with who is entered as the attending provider in SER (Sunrise Enterprise Registration) which is the SHA's Admission/Discharge/Transfer (ADT) system. Requisition stated Tanya Marciniuk; the radiology technologist did not update with correct physician and entered incorrect physician.

- Registration entered incorrect attending physician, ordering provider auto-fills with who is entered as the attending provider in SER. Requisition stated Jeff Marciniuk; the radiology technologist did not update with correct physician and entered incorrect physician.

- Registration entered incorrect attending physician.

- Booking clerk checked in patient without correcting the wrong provider.

- Registration entered incorrect attending physician. Requisition did not have Physician first name/initial, and the registration clerk failed to confirm the physician's first name.

- Physician selection was done in error when a physician name was populated using windows fax and scan, which is the program the Non-Invasive Cardiology department uses to fax documents.

- Doctor selected incorrect physician on Fluency Flex or mobile, which is the 3sHealth self-editing dictation system, at the time of dictation.

- The "Dictated For" doctor was added per audio in the 3s dictation system (though I cannot confirm as it purges after 90 days).

- Dr. Darcy Marciniuk was added as per dictated CC's; the dictating physician requested that Dr. Darcy Marciniuk receive a copy of the report.

- Dr. Darcy Marciniuk was entered as attending at time of registration. When we attached to the visit, this would have triggered that the CC dictated to Dr. Marciniuk to be added.

- Sunrise Clinical Manager (SCM) generated lab order, so someone on ward created the order in SCM with Dr. Darcy Marciniuk. Lab does not receive these requisitions as the ward charts the information on their side, and it is electronically mapped to create an order in lab. The lab has no control over how/when/who generates these orders. (SCM is the electronic medical record).

- Lab generated order, so a paper requisition was served to the laboratory to create this order, however if the label was printed from SCM with Darcy Marciniuk's name on it, lab has no way to know if that was appropriate or not.

[66] In terms of the factors that contributed to the breach, SHA asserted that they included not verifying the first name of the physician, not following procedure for verifying the physician, the physicians full name not being listed by the provider and the fact that there are multiple physicians with the same last name in Saskatoon.

[67] With respect to investigation file 229-2023, the privacy office stated that they first learned of the privacy breaches when contacted by my office on September 29, 2023. In this case, the breaches occurred between October 2021 and July 2023 and affected 11 individuals.

[68] The privacy office commenced its investigation on December 1, 2023. During its investigation, the privacy office contacted the managers in the relevant departments who were asked to investigate. The privacy breaches occurred within La Loche Health Centre and SHA's lab department.

[69] The circumstances of the La Loche Health Centre breach were that a physician dictated a letter and identified the recipient as Dr. DM when they should have identified the recipient as Dr. JM. Therefore, although the letter was sent by fax, the problem was caused when the physician involved didn't identify the correct recipient.

[70] SHA was not able to identify the cause of the breaches involving the SHA lab. It stated that the lab no longer had the requisitions for the lab test and without them it could not determine what had transpired. SHA believes that the factors that contributed to the breach included not verifying the first name of the physician, not following procedure for selecting and verifying the correct physician, and that there are three physicians with the same last name that practice in Saskatoon.

[71] I find that SHA investigated the privacy breaches.

***Take appropriate steps to prevent future breaches***

[72] Prevention is one of the most important steps. A privacy breach cannot be undone but a trustee can learn from one and take steps to help ensure that it does not happen in the future. Some deficiencies in relation to practices, policies, procedures or training may have been identified during the investigation stage.

[73] In Part III of this Investigation Report, I will set out my analysis of the trustees', other than the SHA, plans to prevent further breaches. I now turn to an analysis of SHA's effort to prevent further breaches.

**SHA**

[74] Regarding measures to be taken to prevent further breaches of this kind, SHA asserted that it developed a new "Privacy Training Module for March 2023" which is mandatory. It did not say whether the training module addressed errors of this nature. Nor did it suggest that the training would be provided on an annual basis. It added:

> The SHA Privacy Office is developing a new learning module - *Privacy Education for Managers*. The SHA has developed a Customer Service educational video, *Welcoming Clients in the SHA*, for the registration departments to educate both staff and patients. Manager of Non-Invasive Cardiology stated they are taking measures to prevent this ongoing. He has met with staff to ensure ALL entries into the fax system are inclusive of Physician full name, not just surname. He will continue to monitor this. Managers will remind staff to be certain they are selecting the correct physician. Consistent practice of confirming and verifying the provider is correct. Consistently using full name of care provider when making a requisition, referral or dictating. The Privacy Office will offer to review any work standards the departments have.

[75] It appears that some of the measures identified above will address the circumstances surrounding the breaches. However, additional measures are necessary to ensure that the need to protect privacy and confidentiality is at the top of mind for everyone processing personal health information.

[76] I have previously recommended that SHA provide its privacy training to staff who have access to personal health information on an annual basis (see for example Investigation Reports 320-2017, 043-2018, 066-2018, 081-2022). The need for annual privacy training is also set out in my office's *Privacy Breach Guidelines for Trustees*, at page 3. I will discuss this further below.

[77] In addition, SHA did not provide specific information about how it would address the problem of staff and/or managers not reporting misdirected faxes to the privacy office

despite having noted in its *Privacy Breach Investigation Questionnaire* that there "was a gap between front line staff and the privacy office, as the sending department should have contacted Privacy to report the breach…." SHA added that additional education is required but it has not identified how it will do that.

[78] With respect to investigation file 229-2023, SHA asserted that it took the following steps to prevent further breaches:

> The SHA Privacy Office developed a new Privacy Training module in March 2023, which is mandatory for all staff to complete. Privacy directives and bulletins are posted on the SHA Privacy Intranet page. The SHA has developed a Customer Service educational video, *Welcoming Clients in the SHA*, for the registration departments to educate staff.

[79] Further steps to be taken were described as follows:

> The SHA Privacy Office is developing a new learning module - *Privacy Education for Managers*. Consistent practice of confirming and verifying the provider is correct. Managers to remind staff during huddles to be certain they are selecting the correct physician. Consistently using full name of care provider when making a requisition, referral or dictating. The Privacy Office will offer to review any work standards the departments have.

[80] I find that the SHA did not take sufficient steps to prevent future breaches because it did not commit to providing annual privacy training. Nor has it identified the steps to be taken to ensure staff report all misdirected fax breaches to the privacy office. Failure to report the privacy breach to the privacy office within a reasonable time made it difficult to complete the investigations in the case of some faxes. It also meant that affected parties were notified long after the breaches had occurred.

[81] As noted above, previous investigation reports of my office involving SHA and misdirected faxes have identified the importance of privacy training. Adequate privacy training is an important administrative control and best practice. It is important that the training be refreshed on an annual basis.

[82] In response to my recommendation for annual privacy training in Investigation Report 081-2022 and 120-2022, 135-2022, SHA stated:

> The SHA does not accept this recommendation. As per SHA's Privacy and Confidentiality policy, all staff complete privacy training upon hire, and retake it every three years after that. Due to the high volume of SHA staff, it is unrealistic to have all employees complete the mandatory Privacy Training every year. The privacy training modules are available to all staff throughout the year and can be reviewed at any time. In addition, if the review of the Privacy Training needs to be completed, the SHA Privacy Office will make a recommendation regarding same.

[83] Based on the information provided above and, in this investigation, I am not persuaded that annual privacy training is "unrealistic" or not feasible within the SHA. If the privacy training "modules are available to all staff throughout the year and can be reviewed at any time," then it should be easy to implement mandatory annual privacy training. For these reasons, I will repeat recommendations made in previous investigation reports. I recommend that, within 30 days of issuance of this Investigation Report, SHA provide mandatory annual privacy training to all staff who access personal health information.

**SHA plan to address the systemic problem**

[84] SHA's Questionnaires did not identify a plan to address the systemic problem of misdirected faxes. Also, they did not reference previous recommendations made by my office regarding this problem.

[85] I have been calling for the elimination of traditional faxes and for updates on SHA's work to address the systemic faxing problem since my office's February 2, 2022, Investigation Report 045-2021 et al. I received a quarterly report from SHA in response to this investigation report on August 29, 2022. In that quarterly report, SHA stated that it had carried out work on the provincial EMR to address some of the causes of misdirected faxes associated with the EMR's faxing software. SHA also reported that it had established meetings with operational leads from various departments. However, SHA did not provide my office with information about the nature of the work of this group. Nor has it provided my office with an update since August 2022.

[86] In its response to Investigation Report 032-2022, SHA advised my office that it had established a "working group" to address misdirected faxes. In Investigation Report 080-2022, I recommended that SHA provide my office with a copy of any terms of reference for the "working group" and monthly updates on the work. However, in response, SHA stated that it would "continue to update [my] office as improvements are made to our systems that assist in reducing misdirected reports." It would not commit to providing my office with monthly updates.

[87] In response to Investigation Report 081-2022, where I made the same recommendation, SHA stated:

> The task of addressing the systemic problem of misdirected faxes is complicated and requires consultation with our partners in the health care system. The SHA has had to realign the conversations both internally and externally with our partners. We are creating a framework to engage the appropriate stakeholders both internally and externally, but it is unlikely that we will have that framework created within 30 days of the date of this report. We will continue to update your office as improvements are made to our systems that assist in reducing misdirected reports.

[88] In response to a recommendation made in Investigation Report 120-2022, 135-2022, that SHA provide my office with a monthly update on its working group addressing misdirected faxes, SHA stated:

> Work toward improving misdirected faxes within the provincial health system continues. Finding a sustainable and secure method to share information requires consultation and collaboration with many organizations. That work continues and we will continue to report progress on this issue to the Commissioner as required.

[89] Despite these repeated requests for updates on this work, SHA did not provide my office with any information from SHA about progress made to address the systemic issue since its response to Investigation Report 120-2022, 135-2022 sent in August/December 2022.

[90] During this investigation, following receipt of the Questionnaires, my office asked SHA to provide updates on the steps being taken to address the systemic problem. My office also asked SHA to provide us with the number of breaches involving misdirected health records that have been reported to the SHA privacy office since January 2020.

[91] SHA referred again to the training developed for registration staff and its new privacy training module and daily reminders about accurate data entry. It added that efforts are underway by the registration teams to clean up the data regarding health care providers in its "admission/discharge/transfer systems" and this will be completed in the spring. It added that signage reminding patients about the need to provide accurate information regarding their primary care provider was developed and is now displayed.

[92] It also identified the following technical solutions that have or are being rolled out across the SHA:

- Piloting MedDialogue which will enable communication with health care providers through electronic medical records systems and if implemented will avoid the need for traditional faxes.
- Working to provide physicians access to Sunrise Clinical Manager which will also eliminate the need for traditional faxes, email or mail.
- eHealth Saskatchewan and SHA are developing a central intake for certain medical imaging to eliminate the need for faxed requisitions for MRIs and DT scans. Once implemented, the project will be replicated to include other types of requisitions for medical services.
- A medication management system will be implemented in larger acute care facilities to eliminate the need for orders to be sent by traditional fax machine.

[93] SHA also provided my office with access to its Access, Privacy training module and copies of its Work Standards on ADT System Provider Naming Conventions, two sample Privacy Bulletins and a Poster developed for patients.

[94] Some of the fax related breaches in Investigation Report 045-2021 involved facts similar to those at issue here in that communications were being misdirected to physicians with "look alike", same or similar names. In response to my recommendations that SHA continue efforts to identify look-alike and sound-alike physician names, so staff are prompted to double-check that they have selected the correct physician's name, SHA stated:

> The SHA will work with eHealth, vendors and other system partners to determine if electronic systems can include a prompt for look-alike or sound alike provider names.

[95] During this investigation, my office also asked for an update on this work, and as of the date of this Investigation Report, no updates were provided.

[96] I commend SHA for the technical measures it is working on to eliminate the use of traditional fax machines, work to improve the data quality of key directories, the development of a new privacy training module and the use of bulletins to raise awareness about privacy and misdirected faxes. However, I am not persuaded that its plan is sufficient to address the risks. The privacy training plan is not sufficient, and it does not appear to address the requirements to notify the privacy office of breaches involving misdirected faxes and other communications. It also doesn't address the systemic solutions to directories that include physicians with the same or similar sounding last name or where names are incomplete.

[97] For these reasons, I find that SHA's plan to prevent further breaches involving misdirected faxes is not adequate. I will repeat the recommendations made in previous reports.

[98] I recommend that, within 30 days of issuance of this Investigation Report, SHA work to identify look-alike and sound-alike physician names in its electronic directories or address books and build in flags or prompts so staff are aware that they should double-check that they have selected the right recipient.

[99] I recommend that SHA provide my office with monthly updates on its work on misdirected faxes, with the next update to be provided in February 2024.

## III OTHER TRUSTEES

[100] I now turn to consider the other misdirected fax investigations. In the following cases, a physician or employee used a digital fax system to transmit the personal health information. In most cases, the digital fax systems were built into electronic medical record systems that

included a directory of physicians (physician list or address book) with fax numbers accessible through a drop-down menu.

***Investigation File 274-2023 City Centre Family Physicians (CCFP)***

**Summary:** In March of 2023, the results of an echocardiogram were sent to Dr. DM instead of Dr. JM by a physician. Dr. DM's name appears first in CCFP's physician directory, and their name was incorrectly selected as the intended recipient. The privacy officer did not learn of the incident until CCFP was notified by my office in November 2023.

**Notification of affected individual**: CCFP notified the one affected individual after it received notice of this investigation from my office.

**Investigation:** CCFP conducted an investigation to identify the individual responsible for the breach and the cause of the breach. It learned that the physician selected the first physician in the electronic medical record directory with the last name of Marciniuk. The physician responsible for the incident did not report the matter to the privacy officer. The privacy officer did not learn of the breach until contacted by my office.

**Prevention:** CCFP stated that it is updating its address book to ensure that the first and last names, and physicians' specialties are "very noticeable."

**Findings**: I find that a privacy breach occurred. I find that CCFP failed to notify the affected party within a reasonable period of time. I also find that CCFP's response to the breach was appropriate but further steps can be taken.

**Recommendations**: Within 30 days of issuance of this Investigation Report that CCFP: explore ways to insert a warning flag on physicians who share the same or similar sounding last names with other physicians in the directory; ensure that it has a policy in place governing the secure transmission of personal health information; and ensure that it has a policy in place to require physicians and staff to report privacy breaches to its privacy officer at the earliest opportunity.

***Investigation File 275-2023 Kenderdine Medical Clinic (KMC)***

**Summary:** In April 2023, a KMC physician sent laboratory results via fax using KMC's electronic medical records system to Dr. DM when they should have been sent to Dr. JM. The physician involved picked Dr. DM's name from a drop-down list.

**Notification:** KMC's physician notified the affected individual in November 2023 after KMC was made aware of the breach by our office.

**Investigation:** KMC's investigation identified the physician responsible and how the personal health information was misdirected. It identified the need for more training and a specific policy on using the fax.

**Prevention:** Following the investigation, KMC sent notifications to all staff and physicians to exercise care when sending personal health information. It also added a section on safeguards for faxing personal health information to their policy on privacy and security. It plans to review the policy on privacy and security with staff on a semi-annual basis.

**Findings:** I find that a privacy breach occurred. I find that KMC failed to notify the affected party within a reasonable time period. I find that KMC's response to the breach was appropriate, but further steps should be taken.

**Recommendations:** Within 30 days of issuance of this Investigation Report that KMC: explore ways to insert a warning flag on physicians who share the same or similar sounding last names with other physicians in the directory; and ensure that it has a policy in place requiring physicians and staff to report privacy breaches to its privacy officer at the earliest opportunity.

***Investigation File 278-2023 Wall Street Obstetrics and Gynaecology (WSOG)***

**Summary:** A consultation letter was faxed using WSOG's electronic medical record system in June 2023 to Dr. DM by WSOG's transcriptionist. WSOG became aware of the breach a few days later when Dr. DM's office notified them of the breach. At the time of the incident, WSOG did not have a privacy officer. The patient chart stated that the letter was to be sent to Dr. Marciniuk. A first name was not provided. The transcriptionist selected the first Dr. Marciniuk that appeared in the drop-down menu, which was Dr. DM, when the letter should have been sent to Dr. JM. WSOG was advised of the incident within a few days after the fax was sent.

**Notification:** The affected party was not notified of the breach.

**Investigation:** WSOG stated that the root cause of the breach was that it was not aware that there were two doctors with the same last name, same specialty practicing at the same hospital. It stated that to prevent further breaches, it would ask patients for the first name of their physicians and ensure that it is entered in the electronic medical record correctly. It added "pop-ups" on charts where "Dr. Marciniuk" is the physician to prompt staff to add the first name. It stated that no additional safeguards were needed.

**Findings:** I find that a privacy breach occurred. I find that WSOG failed to notify the affected party. I find that WSOG's response to the breach was appropriate although further actions could be taken.

**Recommendations**: Within 30 days of issuance of this Investigation Report that WSOG: notify the affected party; explore ways to insert a warning flag on physicians

who share the same or similar sounding last names with other physicians in the directory; ensure it has a policy in place that requires privacy and security training of physicians and staff on an annual basis; ensure that it has in place a policy setting out the safeguards for the secure transmission of personal health information by fax; and ensure that it has a policy in place requiring physicians and staff to report privacy breaches to its privacy officer at the earliest opportunity.

***Investigation File 277-2023 South Hill Medical Practice (SHMP)***

**Summary:** In June of 2023, a Medical Office Assistant (MOA) was asked to fax personal health information by a physician. The physician did not provide the MOA with a first name for the physician. The MOA selected the first Dr. Marciniuk which appeared in the SHMP's electronic medical record directory, which was Dr. DM, and faxed the record to them. The fax should have been sent to Dr. JM.

**Notification:** SHMP did not notify the affected party of the breach.

**Investigation:** The SHMP Office Manager only learned of the breach when they received notice of this investigation from my office. They completed an investigation and sent a warning to staff involved to slow down and be more careful when sending personal health information.

Following discussions with my office, the SHMP agreed to implement a practice of monthly updates to its physician directory based on updates to be received from the College of Physicians and Surgeons of Saskatchewan. It also agreed to conduct privacy and security training annually, send regular email reminders about privacy and security to all physicians and staff and remind physicians and staff of the need to report any privacy breaches to the Office Manager as soon as possible.

**Findings:** I find that a privacy breach occurred. I find that SHMP failed to notify the affected party. While appropriate steps were taken to respond to the breach, further actions should be taken.

**Recommendations:** Within 30 days of issuance of this Investigation Report that SHMP: notify the affected party of the breach; explore ways to insert a warning flag on physicians who share the same or similar sounding last names with other physicians in the directory; take steps to ensure that its directory of physicians is updated on a monthly basis; provide privacy and security training annually; send regular reminders about privacy and security to all physicians and staff; and ensure that it has a policy in place requiring physicians and staff to report privacy breaches to its privacy officer at the earliest opportunity.

***Investigation Report 299-2023 Herold Road Family Physicians (HRFP)***

**Summary:** In May 2023, a fax was sent to Dr. DM instead of Dr. JM via a digital faxing system by a physician. The physician selected Dr. DM's name from a drop-down menu that includes physicians' first and last names.

**Notification**: The affected individual was not notified.

**Investigation:** HRFP investigation included an examination of the patient chart to confirm that the breach occurred, and the person responsible and how the fax was misdirected. HRPF does not appear to have considered what the root cause of the breach was and how similar breaches might be prevented. Some general policies were provided to my office on the collection, use and disclosure of personal health information. It is not apparent whether any privacy and security training is provided to staff and what specific safeguards are in place to ensure the secure transmission of personal health information.

**Findings:** I find that a privacy breach occurred. I find that HRFP failed to notify the affected party. While HRFP's response to the breach was appropriate, I find that further actions should have been taken.

**Recommendations**: Within 30 days of issuance of this Investigation Report that HRFP: notify the affected party of the breach; explore ways to insert a warning flag on physicians who share the same or similar sounding last names with other physicians in the physician directory; develop a policy on the secure transmission of personal health information by fax; ensure it has in place a policy on steps to be taken by all staff in response to a privacy breach and provide mandatory annual privacy training to all physicians and staff.

***Investigation Report 308-2023 Dr. Colin Pearce***

**Summary:** In March and June of 2023, Dr. Pearce sent two faxes with personal health information about one patient that was intended for Dr. JM to Dr. DM. The faxes were sent via Dr. Pearce's electronic medical record system. Dr. DM's office alerted Dr. Pearce's MOA about the misdirected fax shortly after receiving them. However, Dr. Pearce was not made aware of the incidents until Dr. DM's office advised that a complaint would be filed with my office.

**Notification:** Dr. Pearce notified the affected patient after they received notice of this investigation from my office.

**Investigation:** Dr. Pearce conducted an investigation. They believe that it was the lack of knowledge about the second physician with the same specialty that contributed to the breach. Dr. Pearce stated that they exercise a high degree of caution when sending faxes and work to get accurate information from patients. Dr. Pearce's MOA stated that they were not aware that the misdirected faxes should be reported to Dr. Pearce. In

discussions with my office, Dr. Pearce stated that they would investigate receiving updated physician lists from the CPSS on a monthly basis to ensure that the physician directory is kept up to date.

**Findings**: I find that a privacy breach occurred. I find that Dr. Pearce failed to notify the affected party within a reasonable time. I find the Dr. Pearce's response to the breach was appropriate. However, further actions should be taken.

**Recommendations:** Within 30 days of issuance of this Investigation Report, that Dr. Pearce: explore ways to flag physicians who share the same or similarly sounding last names with other physicians in the physician directory; take steps to regularly update the physician directory; ensure that they have a policy in place on the steps to be taken in response to a privacy breach; and ensure that their staff receive annual training on privacy.

***Investigation File 226-2023 Saskatchewan Cancer Agency (SCA)***

**Summary:** In February and April 2023, SCA sent three faxes intended for Dr. JM to Dr. DM containing the personal health information of one patient. The faxes were sent using a digital fax machine that includes a correspondence list. If a recipient is not on the list, a user can conduct a search and select a recipient on the SCA's Provider Registry System. SCA concluded that an employee had incorrectly selected Dr. DM as opposed to Dr JM from the Provider Registry System. SCA provided my office with a screen shot of the Provider Registry System showing entries for Dr. Darcy Marciniuk, Dr. Jeffrey Marciniuk and Dr. Tanya Marciniuk. The privacy officer learned about this breach after receiving notice of this investigation from my office.

**Notification:** The one affected party was notified after SCA received notice of this investigation from my office.

**Investigation:** SCA's investigation concluded that the breach occurred. One of the employees involved is no longer with SCA. The other employee was spoken to and provided "follow-up education." SCA learned that the employees involved did not enter the incidents in the Agency's incident management system. Also, the employees responsible for the breach did not take adequate care when selecting the intended recipient contrary to current policy such as by confirming that they had the right fax number. Other policies that speak to the collection, use and disclosure of personal health information include a requirement to take reasonable steps to verify the identity of the person to whom information is disclosed. SCA has a specific policy governing the safeguards to be employed when faxing information. Both employees received privacy training in 2022 and reviewed the confidentiality agreement.

SCA has inquired with the systems provider about the possibility of including prompts in their digital fax system to ask the user to confirm any changes before they are implemented. SCA is conducting an organization wide privacy incident management training in January 2024.

**Findings:** I find that a privacy breach occurred. I also find that SCA failed to notify the affected party within a reasonable time. I find that SCA's response to the breach was appropriate. However, further action should be taken.

**Recommendations:** Within 30 days of issuing this Investigation Report that SCA: explore ways to flag physicians who share the same or similarly sounding last names with other physicians in the Provider Registry System' and ensure that its privacy training is mandatory for all staff on an annual basis.

***Investigation File 279-2023 Dr. Dalisizwe Dewa***

**Summary:** In February and July 2023, two faxes involving two different patients that were intended for Dr. JM were sent to Dr. DM by Dr. Dewa's MOA. The MOA is responsible for sending all faxes. The faxes were sent through Dr. Dewa's electronic medical record system. The breaches were discovered within days of having been sent but Dr. Dewa was not informed of the breaches until November 2023 when he was contacted by our office.

**Notification:** The two affected individuals were notified by telephone.

**Investigation:** Dr. Dewa learned of the breach when the MOA advised him that the matter had been reported to the IPC by Dr. DM's office. The root cause of the breach was "inattention to the first and last name of the physician." As a result of the breach, Dr. Dewa has done a complete review of the privacy policies and practices and issued reminders about privacy to all staff. In addition, staff have added the full first names of the two doctors in their physician directory. Previously, only the first initial of the physician was included in the first name field.

**Findings:** I find that a privacy breach occurred. I find that Dr. Dewa failed to notify the affected parties within a reasonable time. I find that Dr. Dewa's response to the breach was appropriate. However, further action should be taken.

**Recommendations:** Within 30 days of issuance of this Investigation Report that Dr. Dewa: designate one staff person responsible for maintaining the physician directory in the electronic medical record system; explore ways to flag physicians who share the same or similarly sounding last names with other physicians in the electronic medical record system; ensure that there is a policy in place on the steps to be taken in response to a privacy breach; and ensure that privacy training is provided annually to all staff.

[101] In the following investigation, a fax was misdirected to Dr. DM which should have been sent to Dr. TM.

***Investigation Report 280-2023 Willowgrove Medical Group (WMG)***

> **Summary:** In April of 2022, a fax was misdirected via WMG's electronic medical system. The fax was intended for Dr. TM but was sent to Dr. DM. The breach occurred when a transcriptionist was asked to send a copy of a consultation letter to "Dr. Marciniuk." As the transcriptionist no longer works for WMG, WMG presumed "that she did not check to see, or did not know, that there was more than one Dr. Marciniuk." If the transcriptionist had checked the patient chart, they would have seen that the patient's physician was Dr. TM. The first time the privacy officer heard about the breach was when they received notification of the investigation from my office in November 2023.
>
> **Notification:** The affected individual was notified.
>
> **Investigation:** WMG acknowledged the breach and agreed that more privacy safeguards were required. It stated that the root cause of the breach was a lack of attention to detail and failure to follow procedure. To prevent similar breaches in the future, WMG updated its "Fax Policy and procedures", physicians and staff will be made aware that they need to provide specific instructions to staff; it may designate one person to send all the faxes; it will inquire about adding a flag to the physician directory for physicians with the same last name, and staff meetings to be scheduled every two months that will be used for raising awareness of privacy risks. WMG will continue to ask employees to sign confidentiality agreements and provide privacy training every six months.
>
> **Findings**: I find that a privacy breach occurred. I find that WMG failed to notify the affected party within a reasonable time. I find that WMG's response to the breach was appropriate. However, further actions should be taken.
>
> **Recommendations:** Within 30 days of issuance of this Investigation Report that WMG: take the proposed actions described above; and consider designating a staff person to ensure that its physician directory is up to date and accurate.

[102] The following two investigations involve two faxes that were sent via a digital fax system and three that were sent using a traditional fax machine.

***Investigation Files 228-2023 and 268-2023 Prince Albert Co-operative Health Centre (PACHC)***

> **Summary**: Two faxes containing spirometry reports were sent by a nurse on March 14, 2023, using an e-faxing system. The faxes were intended for Dr JM but were sent instead to Dr. DM. Three additional faxes were sent by the same nurse on March 15, 2023, to Dr. DM using a traditional fax machine. The faxes should have been sent to Dr. JM.

The nurse identified the appropriate recipient from a list of physicians on call. The "on call list" identified "J. Marciniuk" as the correct recipient. When the nurse checked the e-faxing system for J. Marciniuk's name and fax number, they could only find an entry for "D. Marciniuk". The nurse sent the reports to Dr. DM assuming that the difference in the first initial was a clerical error.

The nurse was subsequently made aware of the misdirected faxes by Dr. DM's office, but they did not notify the Executive Director of PACHC of the incident contrary to PACHC policy.

**Notification:** Four affected parties were notified once the Executive Director of the PACHC was made aware of the breaches by my office. The fifth affected party has not been notified because their current address is unknown.

**Investigation:** The investigation revealed that the nurse was not following the faxing process and policy "Transmission of Personal Health Information by Fax" which required the nurse to contact the physician involved to confirm the full name and fax number. After becoming aware of the breach, the nurse failed to report it to the Executive Director contrary to PACHC policy. PAHCH concluded that the nurse would have benefited from annual training.

To prevent further breaches, relevant policies have been reviewed and updated. In addition, the related processes for sending reports to doctors on the "on call list" are being revised. Following discussions with my office, PACHC agreed to review the process for updating the physician directory in its electronic medical record system.

Staff responsible for faxing personal health information are now required to annually review the faxing process, policy on the use of fax and the policy related to breach response.

**Findings**: I find that a privacy breach occurred. I find that PACHC failed to notify the affected parties within a reasonable time. I find that PACHC's response to the breach was appropriate. However, further action is required.

**Recommendations**: Within 30 days of the release of this Investigation Report that PACHC: take steps to ensure that its directory of physicians in its electronic medical system is kept up to date and accurate; and implement its plan to improve training on privacy, confidentiality, breach response and the transmission of personal health information by fax.

[103] In one case, the personal health information was sent to Dr. DM instead of Dr. JM via regular mail. A description of the circumstances of that case and my findings and recommendations follow:

***Investigation File 227-2023 Ministry of Health (Health)***

**Summary:** In July 2023, an employee with Health's SAIL Oxygen Program mailed a letter relating to one individual to Dr. DM when it should have been sent to Dr. JM. Dr. DM sent a fax to the branch advising that the letter had been sent to them in error. The Health employee that received the fax from Dr. DM updated the SAIL Oxygen Information System on August 21, 2023. However, the employee did not notify the supervisor of the incident. The Chief Privacy Officer of Health learned of the breach in September from my office.

**Notification:** Health attempted to notify the affected individual by telephone on three occasions. On the third occasion a message was received that the number requested could not be dialed. Therefore, Health did not notify the affected party.

**Investigation:** Health completed an investigation and determined that the mailing address for the physician was obtained from the client's file in Health's Oxygen Information System. When the client file was created, the incorrect treating physician was added. Dr. DM's name was chosen from a drop-down menu or the physician directory instead of Dr. JM's name. To reduce the risk of this happening again, an email was sent to staff in the business unit describing the breach and reminding them to exercise caution and check their work. The email advised them that optional privacy training was available to them. Further monitoring will take place to determine if additional safeguards are required.

Health advised my office that the employee involved received privacy training when initially hired 5 years ago. They were also provided information about breaches and breach management "as breaches occurred."

**Findings**: I find that a privacy breach occurred. I also find Health's failed to notify the affected party within a reasonable time. I find that Health's response to the breach was appropriate. However, further action is required.

**Recommendations:** Within 30 days of issuance of this Investigation Report that Health: explore ways to flag physicians who share the same or similarly sounding last names with other physicians in the Oxygen Information System physician directory; and implement a program of mandatory annual privacy including privacy breach response training for all staff who process personal health information.

## IV FINDINGS

[104] I find that I have jurisdiction to conduct these investigations.

[105] I find that privacy breaches occurred.

***SHA***

[106] I find SHA took some steps to respond to the privacy breaches. However, some additional steps are needed as outlined in the recommendations below.

[107] I find that SHA's notifications to the affected parties were not adequate.

[108] I find that SHA investigated the privacy breaches.

[109] I find that SHA's did not take sufficient steps to prevent further breaches.

***OTHER TRUSTEES***

[110] I find that the other trustees took some steps to respond to the breach. However, some additional steps are needed as outlined in the recommendations below.

## V RECOMMENDATIONS

***SHA***

[111] I recommend that SHA complete its notifications of affected parties within 30 days of issuance of this Investigation Report.

[112] I recommend that SHA revise the draft work standard on notification within 30 days of issuance of this Investigation Report to require a statement about the right to complain to my office.

[113] I recommend that SHA proactively report all misdirected fax breaches to my office beginning within 30 days of issuance of this Investigation Report.

[114] I recommend that, within 30 days of issuance of this Investigation Report, SHA provide mandatory annual privacy training to all staff who access personal health information.

[115] I recommend that, within 30 days of issuance of this Investigation Report, SHA work to identify look-alike and sound-alike physician names in its electronic directories or address books and build in flags or prompts so staff are aware that they should double-check that they have selected the right recipient.

[116] I recommend that SHA provide my office with monthly updates on its work on misdirected faxes, with the next update to be provided in February 2024.

***Other Trustees***

[117] I recommend that, within 30 days of issuance of this Investigation Report, CCFP:

a) explore ways to insert a warning flag on physicians who share the same or similar sounding last names with other physicians in the directory

b) ensure that it has a policy in place governing the secure transmission of personal health information and

c) ensure that it has a policy in place to require physicians and staff to report privacy breaches to its privacy officer at the earliest opportunity.

[118] I recommend that, within 30 days of issuance of this Investigation Report, KMC:

a) explore ways to insert a warning flag on physicians who share the same or similar sounding last names with other physicians in the directory and

b) ensure that it has a policy in place requiring physicians and staff to report privacy breaches to its privacy officer at the earliest opportunity.

[119] I recommend that, within 30 days of issuance of this Investigation Report, WSOG:

a) notify the affected party of the breach

b) explore ways to insert a warning flag on physicians who share the same or similar sounding last names with other physicians in the directory

c) ensure it has a policy in place that requires privacy and security training of physicians and staff on an annual basis

d) ensure that it has in place a policy setting out the safeguards for the secure transmission of personal health information by fax and

e) ensure that it has a policy in place requiring physicians and staff to report privacy breaches to its privacy officer at the earliest opportunity.

[120] I recommend that, within 30 days of issuance of this Investigation Report, SHMP:

a) notify the affected party of the breach

b) explore ways to insert a warning flag on physicians who share the same or similar sounding last names with other physicians in the directory

c) SHMP take steps to ensure that its directory of physicians is updated on a monthly basis

d) provide privacy and security training annually

e) send regular reminders about privacy and security to all physicians and staff and

f) ensure that it has a policy in place requiring physicians and staff to report privacy breaches to its privacy officer at the earliest opportunity.

[121] I recommend that, within 30 days of issuance of this Investigation Report, HRFP:

a) notify the affected party of the breach

b) explore ways to insert a warning flag on physicians who share the same or similar sounding last names with other physicians in the physician directory

c) develop a policy on the secure transmission of personal health information by fax

d) ensure it has in place a policy on steps to be taken by all staff in response to a privacy breach and

e) provide mandatory annual privacy training to all physicians and staff.

[122] I recommend that, with 30 days of issuance of this Investigation Report, SCA:

a) explore ways to flag physicians who share the same or similarly sounding last names with other physicians in the Provider Registry System and

b) ensure that its privacy training is mandatory for all staff on an annual basis.

[123] I recommend that, within 30 days of issuance of this Investigation Report, Dr. Colin Pearce:

a) explore ways to flag physicians who share the same or similarly sounding last names with other physicians in the physician directory

b) take steps to regularly update the physician directory and

c) ensure that they have a policy in place on the steps to be taken in response to a privacy breach and ensure that their staff receive annual training on privacy.

[124] I recommend that, within 30 days of issuance of this Investigation Report, Dr. Dalisizwe Dewa:

a) designate one staff person responsible for maintaining the physician directory in the electronic medical record system

b) explore ways to flag physicians who share the same or similarly sounding last names with other physicians in the electronic medical record system

c) ensure that there is a policy in place on the steps to be taken in response to a privacy breach and

d) ensure that privacy training is provided annually to all staff.

[125] I recommend that, within 30 days of issuance of this Investigation Report, WMG:

a) take the actions described above in paragraph [101] and

b) consider designating a staff person to ensure that its physician directory is up to date and accurate.

[126] I recommend that, within 30 days of issuance of this Investigation Report, PACHC:

a) take steps to ensure that its directory of physicians in its electronic medical system is kept up to date and accurate and

b) implement its plan to improve training on privacy, confidentiality, breach response and the transmission of personal health information by fax.

[127] I recommend that, within 30 days of issuance of this Investigation Report, Health:

a) explore ways to flag physicians who share the same or similarly sounding last names with other physicians in the Oxygen Information System physician directory and

b) implement a program of mandatory annual privacy including privacy breach response training for all staff who process personal health information.

Dated at Regina, in the Province of Saskatchewan, this 17th day of January, 2024.

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