Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 269-2016 & 303-2016

WPD Ambulance and Prairie North Regional Health Authority

March 21, 2017

Summary: A complaint was made against WPD Ambulance (WPD). The Complainant alleged that a WPD employee took a picture of her injury after she had been transferred to the care of a hospital operated by the Prairie North Regional Health Authority (Prairie North). The Complainant was dissatisfied with WPD's response, which included an apology and discipline of the employee in question. The Commissioner investigated what safeguards WPD and Prairie North had in place at the time of the incident. He found that there were not adequate safeguards in place and made several recommendations.

I BACKGROUND

[1] On August 10, 2016, the Complainant was involved in an accident in which she badly injured a portion of her hand. WPD Ambulance (WPD) attended to her injury and transported her to a hospital in Prairie North Health Region for care. While the Complainant was in the hospital, one of WPD's Paramedic took a photograph of the Complainant's exposed, injured hand.

[2] The Complainant made a complaint to WPD. In response, WPD admitted that the taking of the photograph was not in accordance with *The Health Information Protection Act* (HIPA) and issued an apology. The Complainant was not satisfied with WPD's response as it did not indicate what kind of disciplinary actions were taken with respect to the Paramedic.

[3] The Complainant also inquired about the incident with the Prairie North Regional Health Authority (Prairie North). She made a complaint to my office on November 22, 2016. On November 23, 2016, my office notified WPD and the Complainant of my intention to undertake an investigation.

[4] During my investigation of WPD, I found it necessary to examine the safeguards in place by Prairie North. On December 21, 2016, my office provided notification to Prairie North that my office would also investigate its role in this situation.

II DISCUSSION OF THE ISSUES

1. Does HIPA apply in these circumstances?

[5] HIPA applies when three elements are present. The first element is personal health information, the second element is a trustee, and the third element is the personal health information in the custody or control of the trustee.

[6] 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;

[7] The photograph of the hand qualifies as personal health information pursuant to subsections 2(m)(i) and (iv)(A) of HIPA.

[8] WPD submits that the photograph did not qualify as personal health information because it did not identify the Complainant. However, the Complainant was identifiable to the Paramedic who took the photograph and showed it to her colleagues. Further, the injury is somewhat unique and this occurred in a smaller community. There is a risk that, either by itself or when combined with other information available to the other paramedics who saw the photograph, the personal health information could enable the Complainant to be identified.

[9] Subsections 2(t)(ii) and (vii) of HIPA define trustee as follows:

> **2** In this Act:
>
> …
> (t) **"trustee"** means any of the following that have custody or control of personal health information:
>
> …
> (ii) a regional health authority or a health care organization;
> …
> (vii) an operator as defined in *The Ambulance Act*;

[10] WPD qualifies as a trustee pursuant to subsection 2(t)(vii) of HIPA. Prairie North qualifies as a trustee pursuant to subsection 2(t)(ii) of HIPA.

[11] The Paramedic in question took the photograph with her personal cellphone. When asked why the Paramedic took the photograph, WPD reported that the Paramedic indicated that she had not seen an injury like this before and that she wanted to use it to help improve her and her colleagues care if they should have to respond to a similar call in the future.

[12] The Paramedic had access to the Complainant at the time that the photograph was taken because of her role as an employee of WPD. Further, WPD requested that the

photograph be deleted and the Paramedic did so. WPD had control of the personal health information.

[13] All three elements are present in these circumstances. Therefore, HIPA is engaged.

[14] While WPD had control of the personal health information in question, Prairie North chose to contract with WPD and allowed WPD employees in its facility. Prairie North also had a duty to protect this personal health information that was collected when the Complainant was in its care. It also has a duty to ensure that no personal health information is unintentionally disclosed to visitors to facilities through eavesdropping or providing opportunities for photographs of individuals in their care to be taken. These duties arise from section 16 of HIPA which provides:

> **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.

2. Did WPD and Prairie North follow best practices in its response to this privacy breach?

[15] In circumstances where there is no dispute that a privacy breach has occurred, the focus for my office becomes one of determining whether the trustee has appropriately handled the privacy breach. In order to be satisfied, my office would need to be confident that WPD took the privacy breach seriously and appropriately addressed it. My office's

resource, *IPC Guide to HIPA*, recommends five best practice steps be taken by a trustee when responding to privacy breaches. These are:

1. Contain the breach;
2. Notify affected individuals and/or appropriate organizations;
3. Investigate the breach;
4. Prevent future breaches; and
5. Prepare a privacy breach report.

[16] I will use these steps to assess WPD's response to the breach.

Best Practice Step 1: Contain the breach

[17] Upon learning that a privacy breach has occurred, trustees should immediately take steps to contain the breach. Depending on the nature of the breach, this can include:

- Stopping the unauthorized practice;
- Recovering the records;
- Shutting down the system that has been breached;
- Revoking access privileges; or
- Correcting weaknesses in physical security.

[18] WPD learned about the breach from a friend of the Complainant on August 11, 2016, the day after the photograph was taken. The Paramedic who took the photograph was on leave when WPD learned of the breach. WPD's Operations Manager spoke with the Paramedic, upon her return, on August 15, 2016 and asked that the photograph be deleted; and I have been informed by WPD that it has been deleted.

[19] The Operations Manager asked if the Paramedic had shown the picture to anyone. She responded that she had only shown it to other WPD colleagues who were involved on the call as well as other WPD employees. The Operations Manager asked if the Paramedic had shared it via text or social media or in other ways. The Paramedic responded that she had not.

[20] WPD contacted all of the staff that had seen the picture to remind them that taking photographs of patients was not acceptable.

[21] I am satisfied that WPD took adequate measures to contain the breach.

Best Practice Step 2: Notify affected individuals and/or appropriate organizations

[22] Notifying an individual that their personal health information has been inappropriately accessed is important for a number of reasons. Not only do individuals have a right to know, they need to know in order to protect themselves from any potential harm that may result from the inappropriate access. Unless there is a compelling reason not to, trustees should always notify affected individuals.

[23] Although the privacy breach was reported to WPD by the Complainant's friend on August 11, 2016, WPD did not follow up with the Complainant to let her know about what occurred and what steps were taken to prevent future breaches. Instead, the Complainant contacted WPD on August 19, 2016 to proceed with her complaint.

[24] WPD indicated that the friend who reported the breach to WPD asked that WPD not contact the Complainant. WPD indicated that this was why it did not notify the Complainant. WPD did not respond when my office asked if it had a written designation from the Complainant which allowed the friend to exercise rights or powers on behalf of the Complainant, pursuant to section 15 of HIPA.

[25] WPD could have also proactively reported the breach to my office. WPD indicated that it received advice from a health region that my office did not need to be contacted. It is true that there is no requirement for trustees to proactively report privacy breaches in this province. However, my office could have offered WPD guidance with respect to its investigation and response to the breach.

[26] Further, WPD provided me with its three page policy entitled *Protection of Personal and Health Information.* It states: "Any collection, access, use, or disclosure of information not complying with this policy shall be reported to General Manager. The General

Manager will then contact the appropriate Health Authority in Saskatchewan or Alberta." It appears that WPD did not initiate communication with Prairie North; however, it did contact the Saskatoon Regional Health Authority for advice. These actions are not in line with WPD's policy.

[27] WPD did not follow best practices with respect to notifying appropriate individuals and organizations of the breach.

Best Practice Step 3: Investigate the breach

[28] Once the breach has been contained and appropriate notification has occurred, the trustee should conduct an internal investigation. The investigation is generally conducted by the trustee's Privacy Officer because they have the appropriate privacy expertise to do so and understand what the relevant privacy legislation requires of their organization. The investigation should address the incident on a systemic basis and should include a root cause analysis. It should also consider whether the safeguards that were in place at the time of the incident were adequate. The investigation should be documented in an internal privacy breach investigation report. At the conclusion of its investigation, the trustee should have a solid grasp on what occurred.

[29] In its letter to my office, WPD indicated that the Paramedic was disciplined. WPD did not indicate why disciplinary measures were taken.

[30] When privacy breaches occur, I would expect trustees to examine HIPA to see what its responsibilities were with respect to safeguarding personal health information and determine what contributed to the breach.

[31] HIPA sets out rules about collection of personal health information. Subsections 23(2) and 24 provide as follows:

> **23**(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.

> **24**(1) A trustee shall ensure that the primary purpose for collecting personal health information is for the purposes of a program, activity or service of the trustee that can reasonably be expected to benefit the subject individual.
>
> (2) A trustee may collect personal health information for a secondary purpose if the secondary purpose is consistent with any of the purposes for which personal health information may be disclosed pursuant to section 27, 28 or 29.
>
> (3) Nothing in this Act prohibits the collection of personal health information where that collection is authorized by another Act or by a regulation made pursuant to another Act.
>
> (4) A trustee may collect personal health information for any purpose with the consent of the subject individual.

[32] As noted, the Paramedic indicated that she took the photograph to use for educational purposes among her colleagues. Sections 24, 27, 28 and 29 of HIPA do not authorize collection of personal health information for these purposes. Subsection 24(4) of HIPA allows a trustee to collect personal health information for any purpose with the consent of the individual. Section 6 of HIPA explains what is required in order to gain consent. The Paramedic did not take these steps before she took the photograph. This was an improper collection of personal health information.

[33] The Paramedic who took the photograph also showed the picture to fellow WPD employees who were not involved in the Complainant's care. This would qualify as a use of personal health information.

[34] Subsections 26(1) and (2) of HIPA provide rules with respect to the use of personal health information as follows:

> **26**(1) A trustee shall not use personal health information in the custody or control of the trustee except with the consent of the subject individual or in accordance with this section.
>
> (2) A trustee may use personal health information:
>
> (a) for a purpose for which the information may be disclosed by the trustee pursuant to section 27, 28 or 29;
>
> (b) for the purposes of de-identifying the personal health information;

(c) for a purpose that will primarily benefit the subject individual; or

(d) for a prescribed purpose.

[35] Again, nothing in HIPA allowed the Paramedic to use the Complainant's personal health information for these purposes. Consent was not obtained. This was an unauthorized use of personal health information.

[36] Section 16(b)(iii) of HIPA imposes a duty on a trustee to protect personal health information within its custody and control from unauthorized access to or use, disclosure or modification. Trustees must establish proper administrative, technical and physical safeguards that will ensure the security of personal health information. Trustees must ensure that they have policies and procedures in place so that employees understand the rules surrounding collection of personal health information and consent, as well as all of the other components of HIPA. They also must ensure its employees are trained and aware of these policies.

i) WPD's Policies and Procedures

[37] My office asked WPD to provide me with a copy of its privacy policies and procedures. WPD provided me with a three page policy entitled *Protection of Personal and Health Information*. The policy addresses access and privacy rules from four pieces of legislation: HIPA, *The Freedom of Information and Protection of Privacy Act* (FOIP), Alberta's *Health Information Act* and *Freedom of Information and Protection of Privacy Act*.

[38] I examined the policy to determine what instructions were provided regarding the collection and use of personal health information. The following excerpts were relevant:

> Authorized Persons collecting, accessing, using, or disclosing information shall do so in accordance with applicable legislation and WPD & Rosthern and District Ambulance policies.
>
> I. I Authorized personnel shall collect and use:
> a) Health information only where the collection of the information relates directly to, and is necessary for, carrying out WPD & Rosthern and District Ambulance's activities and…

> 4.1 Non - Identifying Health or Personal Information may be collected, accessed, used, and disclosed by WPD & Rosthern and District Ambulance, in accordance with the Health Information Act or Freedom of Information and Protection of Privacy Act.
>
> …
>
> Authorized Personnel means individuals providing services or acting on behalf of WPD & Rosthern and District Ambulance who have been granted access to information on a "need to know" basis, including employees, students, volunteers, individuals providing service on contract, and health service providers.

[39] It is extremely important for trustees to identify which privacy laws apply to their organization. First, I note that WPD does not qualify as a government institution for the purposes of our province's FOIP. Further, the portion of the policy that addresses "non-identifying health information" refers to only Alberta laws and does not address what is required by HIPA. I note that WPD is part of a group of EMS companies that operate in both Saskatchewan and Alberta. WPD should have different sets of policies and procedures for those employees who work in Saskatchewan that addresses HIPA only.

[40] After reviewing these passages, I have determined that WPD's policy is too vague to properly instruct its employees on best practices surrounding the collection and use of personal health information. For example, the policy uses the terms "health information", "non-identifying Health or Personal information" and "information". While the policy does define "health information", it is not as robust as the definition as personal health information found in subsection 2(m) of HIPA.

[41] More importantly, the passage "Authorized personnel shall collect and use: a) Health information only where collection of the information relates directly to, and is necessary for, carrying out WPD & Rosthern and District Ambulance's activities" is not detailed enough to reflect the rules surrounding collection and use found in sections 24, 27, 28 and 29 of HIPA. Further, it does not describe consent and how it should be obtained.

[42] The policy only refers to an important privacy principle: "need-to-know". The need-to-know principle is the principle that trustees and their staff should only collect, use or disclose personal health information needed for the diagnosis, treatment or care of an

individual or for other authorized purposes. Personal health information should only be available to those employees in an organization that have a legitimate need-to-know for the purpose of delivering their mandated services. A trustee should limit collection and use of personal health information to what he/she needs-to-know to do his/her job, not collect or use information that is nice to know. This principle is expressed in subsection 23(1) of HIPA which provides:

> **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.

[43] This principle should be explained fully in any trustee's policy and should have been fully understood by the Paramedic who collected and used the personal health information.

[44] It is best practice for trustees to develop a privacy policy based on the requirements of its applicable privacy legislation as they pertain to collecting, using and disclosing personal and/or personal health information, including consent requirements, individual access to information and correction and security safeguards. The *IPC Guide to HIPA* details what should be included in such a policy. Given this incident, the policy should also explicitly state that photographs should not be taken unless authorized by HIPA. The policy should also provide guidelines regarding the use of a personal device for work duties. If a trustee does not have a robust policy, it will be difficult for it to communicate privacy and security practices to its employees, patients, and partners. On the other hand, if a trustee does have a policy in place, it is clearly demonstrating, in part, that it has done its due diligence with respect to privacy and security. Such a policy is required by section 16 of HIPA.

ii) *Requirements imposed by contract with Prairie North*

[45] I also investigated what types of privacy requirements were imposed on WPD as a result of its contract with Prairie North. Prairie North provided me with a copy of the contract that came into effect in April 2011 and appears to have expired. Prairie North indicated that it is currently being revised and is still in effect now.

[46] Its confidentiality provisions provides as follows:

> 5.1 The Contractor shall, both during and after the term of this Agreement, take all reasonable precautions to maintain confidentiality and secure all material and information that is the property of the Regional Health Authority and/or Saskatchewan Health and is in possession or under the control of the Contractor pursuant to this Agreement.
>
> 5.2 The Contractor shall not directly or indirectly disclose or use, either during or following the term of this Agreement, any material or information belonging to the Regional Health Authority and/or Saskatchewan Health pursuant to this Agreement without first obtaining written consent of the Regional Health Authority and/or Saskatchewan Health for such disclosure or use.
>
> 5.3 The Parties agree not to disclose or make available to any Third Party not associated with the Agreement, any specific financial information contained in this Agreement without the consent of the other Party, except as may be required by law, including the provision of *The Freedom of Information and Protection of Privacy Act* and *The Health Information Protection Act* with respect to the disclosure of information by the Regional Health Authority and/or Saskatchewan Health.

[47] The contract does not have clear language about the protection or flow of personal health information. HIPA is only mentioned with respect to financial information contained in the contract. HIPA has no application to the financial information contained in the contract. Further, the obligation imposed by *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP) should be emphasized.

[48] The contract does require that both WPD and Prairie North comply with all federal and provincial legislation and municipal bylaws in performing their obligations under the contract. Further, WPD is required to provide service "in a manner consistent with" specific Prairie North policies that are listed in an Appendix. The relevant policies listed are as follows:

> 8101 Patient Rights, Privacy Protection — Information Protection
>
> 8105 Patient Rights, Privacy Protection — Use and Disclosure for Provision of Care (Circle of Care)
>
> 8106 Patient Rights, Privacy Protection- Disclosure outside the Circle of Care
>
> 8110 Patient Rights, Privacy Protection — Retention-destruction of Records containing personal health information

8111 Patient Rights, Privacy Protection — Privacy Concerns Handling Process

[49] I am disappointed that this contract does not place more emphasis on the protection of personal health information, especially when the employees of WPD will be working on Prairie North's premises. Prairie North should insist that its contractors have adequate safeguards in place before signing agreements with service providers. Further, when personal health information is being collected, used and disclosed among trustees, an information sharing agreement should be in place. Information sharing agreements are described in my office's resource *IPC Guide to HIPA.* I recommend that Prairie North and the new health region that will be created in Saskatchewan to keep this in mind when signing contracts with various contractors.

[50] I note that two of Prairie North's privacy policies refer to the circle of care. In Investigation Report H-2013-001, my office discussed the concept of "circle of care" and how the need-to-know principle is a more effective principle. Further, the need-to-know principle is in line with HIPA. I recommend that Prairie North update its policies. Prairie Northe indicated that it is gradually phasing out the circle of care concept and that its training material now focuses on need-to-know.

iii) Procedures involving WPD staff in Prairie North facilities

[51] Next, my office asked both WPD and Prairie North what the procedure was when WPD delivered an individual to a Prairie North facility. More specifically, my office asked when the WPD employees were finished their duties. Prairie North confirmed that there were no written policies on the matter. I received different answers about what the specific protocols were.

[52] WPD reported that:

> Once the crew arrives at the hospital they give a verbal report to the receiving hospital staff and transfer care to the RN or Doctor. The ambulance staff then complete their patient care report and often return to base. It is not uncommon for the crew to stay at the hospital and help with patient care if asked to do so.

[53] The Lloydminster Hospital Emergency Department Manager indicated that the emergency medical services (EMS) staff is part of the care team and at times will help stabilize patients. So they are allowed in the emergency room but only if their assistance is needed. He did not indicate who makes that call.

[54] The Director of Emergency Health Services at Prairie North explained that it is common practice for EMS staff to continue to assist with care and make contact with the patient and family once in the emergency room in order to collect personal health information that they were not able to get *en route* to the hospital. He noted that this occurs most often in serious situations. He also noted that "They stay up-to-date with care provided and just assist because sometimes it is appreciated by ER staff." Finally, he noted that in the situation in question, the same crew had transferred the patient to a tertiary center or Airport for an Air Ambulance transfer, it was reasonable for the Paramedic to make subsequent contact with the patient in the patient's room or bed area.

[55] Finally, the Vice President who is responsible for EMS reported that WPD is contracted to provide pre-hospital ambulance care. She also noted that EMS crew might assist in transferring patients on to an emergency room stretcher and might stay until a patient is stabilized.

[56] The lack of a formal written protocol is troublesome from a privacy stand point. It would be difficult for an employee to determine if he or she had a need-to-know personal health information if he or she did not know when his or her role ends. Further, if EMS staff are involved in the collection of personal health information, it should be clear when it is appropriate to do so and for what purpose. In general, it appears personal health information is routinely being collected by one trustee and disclosed to another. No information sharing agreement is currently in place to clarify the roles in this situation. The ambiguity in these protocols may have contributed to the Paramedic's lack of understanding about when it was appropriate for her to access the Complainant and collect her personal health information (take a picture).

[57] WPD indicated that such a protocol would be difficult to write and would be difficult to apply from patient to patient. Prairie North did not disagree with my recommendation to establish such a protocol.

iv) Personal health information routinely collected by WPD

[58] My office asked what personal health information is collected by WPD and Prairie North when EMS staff have finished their duties. WPD reported that there is a provincial Patient Care Report (PCR) form that is filled out for each patient and left at the hospital on the patients hospital chart. A copy of this report is collected by WPD. There is no written policy or agreement between WPD and Prairie North to address this. WPD indicates that this is collected for quality of care purposes. The form collects the following data which constitutes personal health information pursuant to subsection 2(m) of HIPA: name, home address, medical complaint and findings, past medical history, treatment, next of kin, telephone numbers and health cards. WPD should have a policy in place addressing WPD's authority to collect and use these PCRs and how they will be safeguarded.

[59] Another important privacy concept is the data minimization principle. It means that a trustee should collect, use or disclose the least amount of identifying information necessary for the purpose. This is also enshrined in section 23 of HIPA.

[60] As per subsection 23(1) of HIPA, trustees are required to only collect as much personal health information as is required for the purpose for which it is collected. WPD should revise its practices with respect to the collection of all of the personal health information on the provincial PCR form to ensure it respects the data minimization principle.

v) WPD training regime

[61] Finally, my office asked WPD to describe the privacy training given to its paramedics. It simply reported that new hires are asked to sign a New Employee Confidentiality Agreement and WPD keeps this on the employee file. It also noted that paramedics are taught at school about the protocol regarding the PCRs that are left at the hospital and returned to WPD.

[62] I am not satisfied that WPD has provided adequate privacy training to its employees, including the Paramedic in question. WPD does not have adequate policies regarding the protection of personal health information. There are no protocols and information sharing agreements in place between WPD and Prairie North. Finally, WPD did not explain how it ensures its employees are familiar with and follow Prairie North's policies as required by the contract. It is best practice for trustees to have robust policies and procedures in place and have An annual mandatory training program to ensure employees are familiar with these safeguards. Training should occur when staff members are first hired and again once every year. This is what is required to meet the duty imposed on WPD by subsection 16(c) of HIPA.

[63] I am not satisfied that WPD fully investigated this breach. It was quick to place blame on and discipline the Paramedic in question. As a result of my investigation I have found that WPD and Prairie North did not have reasonable safeguards in place that could have prevented this breach. These lack of safeguards include:

- WPD's privacy policy was inadequate and addresses Alberta's legislation;
- there were not proper agreements in place between WPD and Prairie North addressing the protection of personal health information;
- there were ambiguous expectations of the EMS staff when transferring patients to Prairie North care;
- Prairie North's policy uses an outdated circle of care model while WPD's policy uses the need-to-know principle; and
- WPD does not provide adequate privacy training to its staff.

Best Practice Step 4: Prevent future breaches

[64] The final step is to formulate a plan to avoid future breaches of a similar nature. Some changes that are needed may have revealed themselves to the trustee during the investigation phase, such as deficient policies or procedures, a weakness in the system, a lack of accountability measures or a lack of training. This is an important step in

addressing a privacy breach because a privacy breach cannot be undone but the trustee can learn from it and improve.

[65] WPD reported that its plan for prevention was to discipline the Paramedic in question and to discuss the situation with all of its staff members.

[66] It was appropriate to discuss the incident with staff of WPD, and of the two EMS companies also owned by its parent company, in a manner that protected the identity of both the Paramedic and the Complainant.

[67] However, given the incomplete investigation on the part of WPD, they have not provided a plan for prevention to address the lack of safeguards. I have made a number of recommendations at the end of this report that WPD should implement.

Best Practice Step 5: Prepare a privacy breach report

[68] WPD provided a letter to my office explaining the steps it took in response to the breach. It also responded to questions from my office. It did not follow best practices by preparing and submitting a final report.

[69] I suggest that the new health entity, when created, consider the recommendations in this report and implement them on a province wide basis.

III FINDINGS

[70] I find HIPA applies in these circumstances.

[71] I find that WPD did not follow best practices when responding to the breach.

IV RECOMMENDATIONS

[72] I recommend that WPD develop a more detailed, compliant privacy policy that addresses the subjects described on page 160 of the *IPC Guide to HIPA* and described in this report.

[73] I recommend that WPD's privacy policy create a separate privacy policy for employees in Saskatchewan.

[74] I recommend that WPD revise its practices with respect to the collection of all of the personal health information on the provincial PCR form.

[75] I recommend that WPD and Prairie North revise its agreement and ensure it contains all elements found in an information sharing agreement.

[76] I recommend that WPD and Prairie North develop a procedure regarding the role of EMS staff on the premises of the region.

[77] I recommend that Prairie North revise its policies and replace the circle of care model with the need-to-know principle.

[78] I recommend that Prairie North insist that its contractors have adequate safeguards for the protection of personal health information in place before providing service.

[79] I recommend that WPD develop a robust privacy training program for its employees which includes an annual review of its policies as well as Prairie North policies.

[80] I recommend that WPD's parent company apply these recommendations to all its EMS companies operating in Saskatchewan.

[81] It is difficult to give recommendations to an entity that has not yet been created but I would encourage the new single health authority to take the above recommendations into account when it enters into contracts with ambulance service companies and in developing its policies regarding transfer of personal health information from one trustee to another trustee.

Dated at Regina, in the Province of Saskatchewan, this 21st day of March, 2017.

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