Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 021-2017, 067-2017 & 068-2017

Medstar Ventures Inc. operating as North-East EMS, Saskatchewan College of Paramedics & Ministry of Health

August 17, 2017

Summary: This Investigation Report tracks how the personal health information of 10 individuals was collected, used and disclosed by three trustees as it moved through the health system. The Commissioner found that North-East EMS did not have reasonable safeguards in place. As a result, an employee disclosed the personal health information to the Saskatchewan College of Paramedics (the College) without authorization. The College's collection of the personal health information was not authorized due to the unauthorized disclosure. The College then used the personal health information to collect additional personal health information from the Ministry of Health (the Ministry). The Commissioner also questioned the Ministry's authority to have collected the personal health information. He made several recommendations.

I BACKGROUND

[1] This Report examines how 10 Patient Care Record forms (PCR) made their way through the health system. This investigation was initiated when a privacy breach was proactively reported to my office. PCRs are forms issued by the Ministry of Health and used by paramedics when they respond to a call. Each one has a unique identifying number.

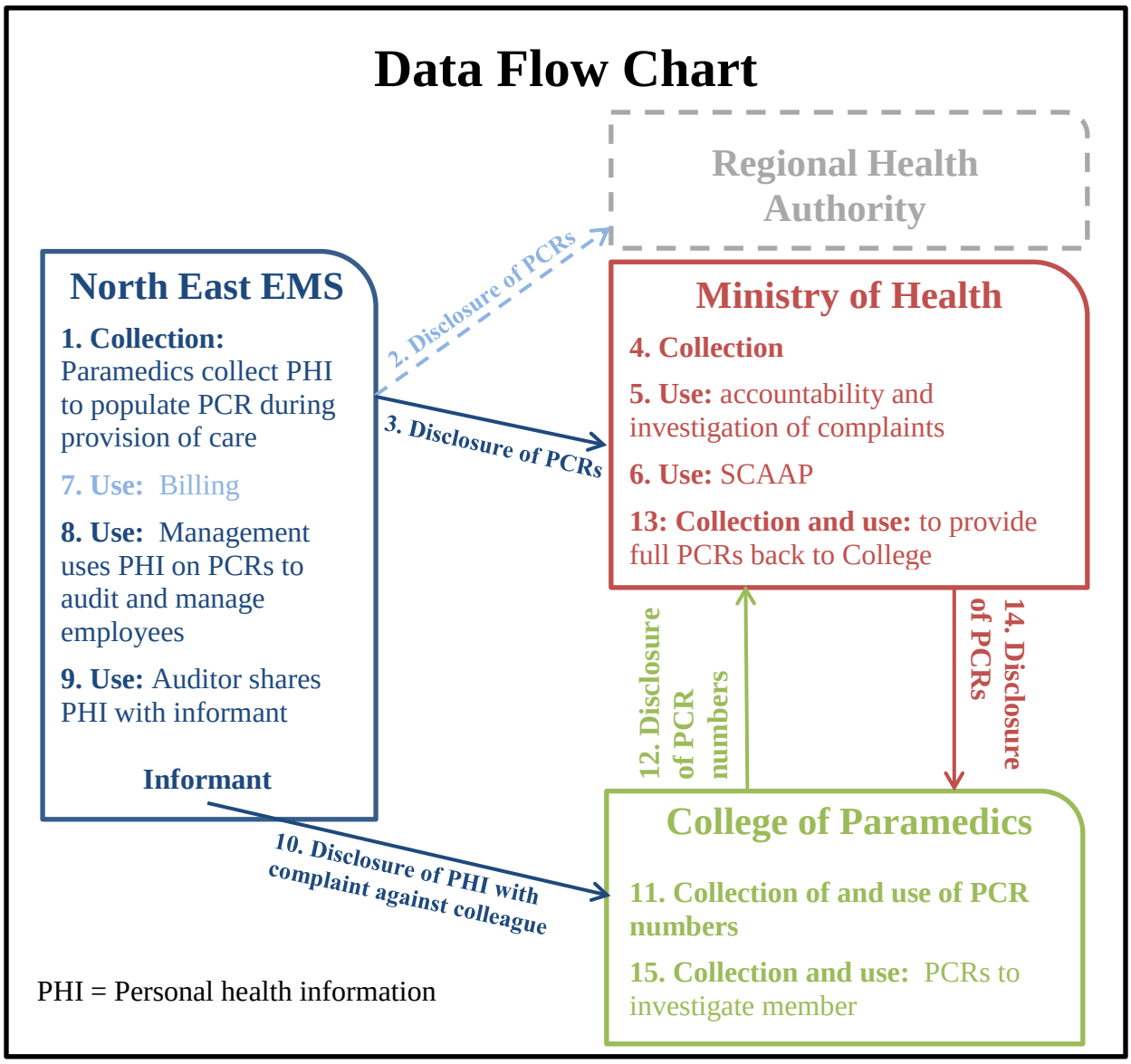
[2] On February 1, 2017, North-East EMS (North East) proactively reported a privacy breach to my office. It indicated that numbers of specific PCRs, and other details on the PCRs had been disclosed to the Saskatchewan College of Paramedics (the College) by an employee (the Informant) as part of a complaint against one of North East's paramedics (the Paramedic).

[3] On February 8, 2017, my office provided notification to North East of my office's intention to undertake an investigation and asked that it provide an internal investigation report to my office.

[4] North East later reported that its investigation efforts were hampered because the College refused to disclose the name of the Informant.

[5] On March 13, 2017, my office met with representatives from the College. The College explained its role in the complaint and its use of the PCR numbers and other information on the forms. It indicated that it collected the PCRs in question from the Ministry of Health (the Ministry). I was concerned with the flow of personal health information in these events. On April 7, 2017, my office advised both the College and the Ministry that my office would also investigate their roles in these data transactions.

[6] The data flow chart on the next page describes how the personal health information in question moved through the system. Each numbered item represents a data transaction involving personal health information.


Data Flow Chart
Regional Health Authority
North East EMS
1. Collection: Paramedics collect PHI to populate PCR during provision of care
7. Use: Billing
8. Use: Management uses PHI on PCRs to audit and manage employees
9. Use: Auditor shares PHI with informant
Informant
2. Disclosure of PCRs
3. Disclosure of PCRs
Ministry of Health
4. Collection
5. Use: accountability and investigation of complaints
6. Use: SCAAP
13: Collection and use: to provide full PCRs back to College
12. Disclosure of PCR numbers
14. Disclosure of PCRs
10. Disclosure of PHI with complaint against colleague
College of Paramedics
11. Collection of and use of PCR numbers
15. Collection and use: PCRs to investigate member
PHI = Personal health information

II DISCUSSION OF THE ISSUES

1. Does HIPA apply in these circumstances?

[7] *The Health Information Protection Act* (HIPA) applies in full when three elements are present. The first element is personal health information, the second element is a trustee, and the third element is if the personal health information is in the custody or control of the trustee.

[8] 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;

[9] Registration information is defined by subsection 2(q) of HIPA as follows:

> 2 In this Act:
> …
> (q) "registration information" means information about an individual that is collected for the purpose of registering the individual for the provision of health services, and includes the individual's health services number and any other number assigned to the individual as part of a system of unique identifying numbers that is prescribed in the regulations;

[10] At issue is the information contained in 10 PCRs that were used to assess the Paramedic's performance.

[11] The Ministry explained that, in general, PCRs were developed and are administered by the Acute and Emergency Services Branch of the Ministry. They are used by all the ground ambulance services within the province when answering a call.

[12] PCRs identify the patient and provide registration information. This qualifies as personal health information pursuant to subsection 2(m)(v) of HIPA. PCRs provide a history of the patient's condition and complete account of the care provided by the paramedic. The PCR also contains billing information, trip record data, assessment data, and pickup and destination information. This information qualifies as personal health information pursuant to subsections 2(m)(i), (ii) and (iv) of HIPA.

[13] Further, the PCRs also contain a unique identifying number. Specifically, these numbers qualify as personal health information because they fit within the definition of personal health information provided by subsection 2(m)(iv) of HIPA. As discussed later in this Report, these numbers have the ability to re-identify subject individuals as described in subsection 3(2) of HIPA which provides:

> 3(2) This Act does not apply to:
>
> > (a) statistical information or de-identified personal health information that cannot reasonably be expected, either by itself or when combined with other information available to the person who receives it, to enable the subject individuals to be identified;

[14] Next I will determine if there are trustees involved. Trustee is defined in subsection 2(t) of HIPA. Relevant portions are as follows:

> 2 In this Act:
> …
> (t) "trustee" means any of the following that have custody or control of personal health information:
>
> > (i) a government institution;
> > …

> (vii) an operator as defined in *The Ambulance Act*;
> …
> (xiii) a health professional body that regulates members of a health profession pursuant to an Act;
> …

[15] The Ministry qualifies as a trustee pursuant to subsection 2(t)(i) because it is a government institution as defined by subsection 2(1)(d)(i) of *The Freedom of Information and Protection of Privacy Act* (FOIP).

[16] North East is an operator as defined in *The Ambulance Act*; therefore, it qualifies as a trustee pursuant to subsection 2(t)(vii) of HIPA. Its Provincial Ambulance Licence lists "North East as Medstar Ventures Inc. o/a North-East EMS".

[17] The College is a health professional body that regulates paramedics pursuant to *The Paramedics Act.* The College qualifies as a trustee pursuant to subsection 2(t)(xiii) of HIPA.

[18] Finally, I must determine if these three trustees had custody or control of the personal health information in question. Custody is the physical possession of a record by a trustee, who has a measure of control. Control connotes authority. A record is under the control of a trustee when the trustee has the authority to manage the record, including restricting, regulating and administering its use, disclosure or disposition. Custody is not a requirement.

[19] The data flow chart demonstrates when each trustee had custody of the personal health information in question. Data transaction one indicates that North East had custody of the personal health information first after collecting it directly from patients. Data transaction four indicates that the Ministry had custody of the personal health information when it collected it from North East. Data transactions 11 and 15 indicate that the College had custody of the personal health information when it collected it both from the Informant and the Ministry.

[20] All elements are present and HIPA applies in these circumstances.

2. What is the purpose of the PCR and is it authorized by HIPA?

[21] The Ministry explained that it is responsible for the oversight of ground and air ambulance programs within the province of Saskatchewan. The PCR was developed and is administered by Acute and Emergency Services Branch of the Ministry to fulfill the obligations of record of service reporting described in section 51 of *The Ambulance Regulations* which requires ambulance operators to ensure that a record of service is created for each ambulance response and provided to the Ministry each month.

[22] Section 51 of *The Ambulance Regulations* provide:

> 51(1) Every operator shall:
>
> (a) cause to be prepared, on forms supplied by the minister for the purpose, a written record of service with respect to each call response;
>
> (b) ensure that the portions of a form related to patient identification, history, assessment and treatment are completed immediately on transportation of a patient, and that the balance of the form is completed within 24 hours after the transportation of a patient;
>
> (c) ensure that the copies of each record prepared pursuant to clause (a) are distributed in the manner designated on the form; and
>
> (d) ensure that any copy of a form designated to be distributed to the minister is forwarded to the minister prior to the end of the month following the month in which the form is completed.
>
> (2) Each operator shall retain a copy of the forms described in subsection (1) for a period of 10 years from the date of transportation of the patient.
> …
> (5) On the request of any person with whom the operator has a contractual arrangement with respect to a patient who is eligible to receive benefits from that person, an operator may disclose or communicate the forms completed pursuant to subsection (1) or any information from the forms to the person named in the request.

[23] Subsections 24(2), 26(2)(a) and 27(4)(l) of HIPA authorizes the data transactions described in section 51 of *The Ambulance Regulations* as follows:

> 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.
> …
>
> 26(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;
> …
>
> 27(4) A trustee may disclose personal health information in the custody or control of the trustee without the consent of the subject individual in the following cases:
> …
> (l) where the disclosure is permitted pursuant to any Act or regulation;

[24] North East's collection of the personal health information on the 10 PCRs in question, the first data transaction on the data flow chart, was collected directly from the subject individuals. This collection is authorized both by subsection 24(1) of HIPA and subsections 51(1)(a) and (b) of *The Ambulance Regulations,* which are supported by subsections 24(2) and 27(4)(l) of HIPA.

[25] North East then disclosed the 10 PCRs to both the relevant regional health authority and the Ministry. These disclosures and subsequent collections are represented by data transactions two, three and four on the data flow chart.

[26] The authority of the regional health authority to collect and use the PCRs is not in the scope of this investigation.

[27] The Ministry has indicated that these data transactions were authorized by subsections 24(2) and 27(4)(l) of HIPA and subsection 51(1)(c) of *The Ambulance Regulations* which provides that copies of each PCR be distributed in the manner designated on the form. The PCRs are triplicate carbon forms. The PCRs indicate that the white (original) copy is to be kept on file with the ambulance operator, the yellow copy is to be disclosed to the

"medical records" for the subject individual's file, and the pink copy is to be disclosed to the Ministry.

[28] I note that the yellow page indicates only that it should be submitted to "Medical Records". While it may be understood that this means that the form should be submitted to the relevant regional health authority, the form should be specific. I recommend that the Ministry change the form to make it clear.

[29] The Ministry collects these forms in two ways. They receive the physical pink PCR copy from the operator. All personal health information is collected in this manner. Additionally, the operator is also responsible for entering certain personal health information from the PCRs into the Provincial Ambulance Information System Database. Operators do not enter handwritten notes that appear on the PCR into this database.

[30] The Ministry uses the personal health information on the PCRs for two main purposes. It indicated that the first, data transaction five, is to respond to complaints about ambulance services. The types of complaints include care that was provided, the length of response time, wait times at hospitals, billing concerns and events during their patient care journey.

[31] The Ministry indicated that it is authorized to use personal health information for these purposes pursuant to subsections 26(2)(a), 27(2)(b) and 27(4)(k)(ii) of HIPA which provide:

> 27(2) A subject individual is deemed to consent to the disclosure of personal health information:
>
> …
>
> (b) for the purpose of arranging, assessing the need for, providing, continuing, or supporting the provision of, a service requested or required by the subject individual;
>
> 27(4) A trustee may disclose personal health information in the custody or control of the trustee without the consent of the subject individual in the following cases:
>
> (k) where the disclosure is being made for the purpose of:
>
> …
>
> (ii) planning, delivering, evaluating or monitoring a program of the trustee;

[32] Responding to complaints about care received in the past would not fall under subsection 27(2)(b) of HIPA because it would not qualify as arranging, assessing the need for, providing, continuing, or supporting a future health service.

[33] Responding to complaints about past service provided would fall under subsection 27(4)(k)(ii) of HIPA because it would qualify as evaluation. However, the evaluation must be a program of the trustee.

[34] Complaints about the care received by a paramedic are under the legislative jurisdiction of the College, not the Ministry. Complaints should be referred to the College or the operator. Because it is not a program of the Ministry to manage the actions of paramedics, the Ministry cannot rely on subsection 27(4)(k)(ii) to use personal health information for these purposes.

[35] Regional health authorities are responsible for contracting with ambulance operators to provide emergency medical care. The length of response time, wait times at hospitals and most billing concerns are about programs provided by either a health region or an ambulance operator and, again, are not programs of the Ministry. Again, the Ministry cannot rely on subsection 27(4)(k)(ii) to use personal health information for these purposes.

[36] I recognize that the Ministry provides licences to ambulance operators and has some oversight responsibilities over both the College and regional health authorities. In some situations, the Ministry must be involved in the resolution of complaints. However, the Ministry should follow the data minimization and need-to-know principles and only collect the personal health information if there is a complaint that needs to be addressed by the Ministry.

[37] Section 23 of HIPA requires that all collection, uses and disclosures of personal health information by trustees should be guided by the data minimization and need-to-know principles. Section 23(1) 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.

[38] The data minimization principle means that a trustee should collect, use or disclose the least amount of identifying information necessary for the purpose. 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 other authorized purposes. Personal health information should only be available to those employees in an organization that have a legitimate need-to-know that information. 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.

[39] In addition, responding to complaints regarding response times does not require all of the personal health information collected by paramedics on a PCR. Similarly, personal health information collected by a paramedic should not have any bearing on the amount of time a patient waits at a hospital. Finally, billing is based on a basic call "pick up" rate, a per kilometre rate for rural residents to transfer into larger centres; an hourly waiting time rate to cover the time an ambulance waits in a larger centre to return a patient to his or her home community; and a special escort fee, if needed. In some cases, it also depends on length of time an individual waits for a transfer. It does not depend on any other personal health information collected on the PCR.

[40] The Ministry indicated that the other use, data transaction six, is for the administration of the Senior Citizens' Ambulance Assistance Program (SCAAP) which caps the cost of ambulance services for individuals over the age of 65. This use of personal health information on the PCRs is authorized by subsections 26(2)(a) and 27(2)(b) of HIPA.

[41] However, again, the Ministry does not require all of the personal health information on all PCRs for the purpose of arranging, assessing the need for, providing, continuing, or supporting the provision of SCAAP.

[42] Even though *The Ambulance Regulations* authorizes the Ministry to collect the personal health information on the PCR's, I believe the practice does not recognize the data minimization or need-to-know principles.

[43] I recommend the Ministry reevaluate its need to collect all personal health information on every PCR. I also recommend that the PCR be changed so that the Ministry collects only personal health information needed for the purposes. Perhaps, this could be accomplished by collecting only limited personal health information through the Provincial Ambulance Information System Database. This may also require an amendment to *The Ambulance Regulations.*

[44] In response, the Ministry stated that it had not contemplated how the information could be collected on two forms yet be linked when needed for billing or casework. It noted that this would take a significant overhaul of the system and processes for all stakeholders and would most likely result in significant inefficiencies. I urge the Ministry to study the matter and look for solutions to any challenges that may arise.

3. Did North East have authority to use the personal health information in question?

[45] North East noted that it routinely uses the personal health information it collects on the PCRs in two main ways.

[46] The first use of the personal health information, data transaction seven on the flow chart, is for the purpose of billing for the services it provides, which is not the focus of this investigation.

[47] The second way North East routinely uses the personal health information collected on the PCR's is to audit the performance of its employees. This is depicted by data transaction eight on the data flow chart. North East indicated that an experienced paramedic or advanced care paramedic working for the organization is assigned to this duty. Every PCR is reviewed to ensure that the documentation is complete and that the paramedics took appropriate actions in the performance of their duties. In cases where

there are concerns or where outstanding work is demonstrated, the paramedics involved will receive feedback which is placed on their employee file.

[48] The use of the personal health information to manage the performance of employees is not specifically authorized in HIPA. There are provisions in *The Freedom of Information and Protection of Privacy Act* (FOIP) that allow the use of personal information for these purposes. I find that this would be evaluating and monitoring a program of the trustee and is therefore authorized by subsection 27(4)(k)(ii) of HIPA.

[49] However, North East has indicated that it does not have a written policy, procedure or guidelines with respect to these audits in place. There is no specified timelines and no guidelines on what documentation is produced or kept as a result of the audits. It has indicated that training for the auditors is informal. Most importantly, it does not have guidelines regarding how personal health information can be used or disclosed for the purpose of audits. I recommend that North East develop a policy and procedure respecting the use of auditing PCRs for the purpose of employee management.

4. What happened to the personal health information involved in the audit and did North East have adequate safeguards in place?

[50] During the fall of 2016, North East's Auditor (the Auditor) reviewed the 10 PCRs in question and had concerns about the performance of the Paramedic in question.

[51] On October 5, 2016, the College received an e-mail of complaint against the Paramedic from a different North East paramedic, the Informant. The e-mail contained the form numbers of all 10 PCRs. As discussed earlier, these numbers qualify as personal health information. The e-mail also contained other personal health information about the subject individuals. The Informant's e-mail also indicated that she had never worked with the Paramedic and therefore would not have been part of the treatment of the subject individuals. North East also confirmed the Paramedic was not a part of the audit process, yet the e-mail also provided details of the audit.

[52] The Informant did not have a need-to-know of the personal health information that was in North East's custody.

[53] North East asked both the Auditor and the Informant how the Informant became aware of the personal health information. They both gave conflicting answers at different times. However, recently they have both admitted that the Auditor shared the personal health information with the Informant. North East has admitted that this was an unauthorized use of personal health information, as represented by data transaction nine on the flow chart.

[54] The Informant then disclosed the personal health information to the College (data transaction ten). There are provisions in HIPA which, in appropriate circumstances, authorizes a trustee to disclose personal health information to the College. It is important to note that, in some rare circumstances, a paramedic could qualify as a trustee on their own. However, in this case North East was the Trustee with custody and control of the personal health information in question. The Auditor and Informant are employees of the Trustee. The Informant made the disclosure on the Informant's own accord. Therefore, this was not an authorized disclosure.

[55] When a breach occurs, my office investigates to ensure that the trustee had reasonable safeguards in place as required by 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.

[56] Some of the basic safeguards that I expect every trustee in the province to have in place include a comprehensive set of written privacy policies, the appointment of a privacy officer, annual training for employees, confidentiality agreements signed annually by employees, access restrictions, a records retention schedule, technical safeguards for computer systems (such as user identification and passwords on digital systems) and physical safeguards (such as locked filing cabinets for physical records).

[57] Privacy policies should cover the following topics:

- Accountability for personal health information;
- Purpose for collecting personal health information;
- Consent for collecting, using and disclosing personal health information;
- Accuracy and correction of personal health information;
- Retention and destruction of personal health information (written records retention and disposition schedule);
- Privacy breach management;
- Use and disclosure audits;
- Use and disclosure control;
- Individual access to information;
- Privacy complaint management; and
- Enforcement mechanisms

[58] Policies should also reference the applicable authorities upon which the policy is based – in this case, HIPA. Further, as noted above, North East should have policies addressing specific internal uses of personal health information, such as auditing.

[59] With respect to written policies, North East sent me two relevant policies it had in place at the time of the unauthorized uses and disclosures. The first is a one page policy entitled *Release of Information* and the second is a five page policy entitled *Completion* which details how a PCR form should be completed. Upon review, I find these policies are not comprehensive enough to reasonably meet the standard imposed by section 16 of HIPA. North East's policies did not reference HIPA.

[60] Once a trustee has appropriate privacy policies in place, it should design an annual training program for its employees to ensure that the expectations of the policies and the

duties and consequences of HIPA are well known by employees. Employees should then sign annual confidentiality agreements to signal that they understand their responsibilities.

[61] North East indicated that during its hiring process paramedics are questioned "about the privacy of patients which is learned during paramedic training". It also noted that on a daily basis staff are questioned about calls and they respond appropriately about not giving any patient information. Finally, North East indicated they have begun asking employees to sign a document "where they understand the ramifications of HIPA". This is not a reasonable training regime, especially without comprehensive written policies in place.

[62] North East did not have policies in place to clarify who is accountable for the protection of personal health information. North East did not have policies in place to guide the Auditor or the Informant on what constitutes a use of personal health information and what uses may be authorized by the organization or HIPA. North East did not have policies in place to guide the Auditor or the Informant on what constitutes a disclosure of personal health information and what disclosures may be authorized by the organization or HIPA. The Auditor and Informant did not receive privacy training from North East as required by section 16 of HIPA. North East did not have a policy outlining the audit process and did not provide training to staff about the proper channels for resolving complaints within the organization.

[63] Further, North East did not have a privacy officer in place at the time of the uses or disclosures. Section 58 of HIPA provides:

> **58**(1) Where this Act or the regulations require a decision to be made or an opinion to be formed by a trustee that is a government institution as defined in *The Freedom of Information and Protection of Privacy Act*, the person who is the head, as defined in that Act, of the government institution, or the designate of the head, shall make the decision or form the opinion on behalf of the trustee.
>
> (2) Where this Act or the regulations require a decision to be made or an opinion to be formed by a trustee that is a local authority as defined in *The Local Authority Freedom of Information and Protection of Privacy Act*, the person who is the head,

> as defined in that Act, of the local authority, or the designate of the head, shall make the decision or form the opinion on behalf of the trustee.
>
> (3) Where this Act or the regulations require a decision to be made or an opinion to be formed by a trustee to whom subsection (1) or (2) does not apply, the trustee shall designate a person to make the decision or form the opinion on behalf of the trustee.

[64] As noted, disclosures of personal health information to the College may have been authorized if it had been made by the trustee in some circumstances. However, in this case, there was no one in North East designated to be responsible for these decisions as required by subsection 58(3) of HIPA. The Informant had no one in the organization to consult on whether the disclosure was supported by the organization.

[65] I am not satisfied that North East had reasonable safeguards in place as required by section 16 of HIPA. In particular, North East did not ensure compliance with HIPA by its employees as required by subsection 16(c) of HIPA. I recommend that North East implement all of the safeguards discussed in this report in its organization.

[66] The Auditor and the Informant have to take some responsibility for their actions. North East alleges that the Auditor's concerns were not brought to the attention of North East's management until December 2016, after the Complaint was sent to the College. Management then addressed these concerns with the Paramedic. If the Auditor had concerns about a co-worker, he should have raised it with management. If North East's management failed to take adequate steps, then the Auditor should have gone directly to the College without personal health information to discuss his concerns and next steps, not to a co-worker who had no authority to resolve the situation. Similarly, the Informant had no authority to disclose the personal health information to the College. I note that North East has terminated the Auditor because of these actions.

5. Did the College have authority to collect and use personal health information from the Informant?

[67] The College is the licencing body for paramedics in the province of Saskatchewan. It is mandated through *The Paramedics Act*. Part of its mandate is to regulate and discipline

members. When a complaint is received involving a paramedic, a professional conduct committee is authorized by section 27 of *The Paramedic Act* to investigate the matter. Subsection 27(1) of *The Paramedics Act* provides:

> 27(1) Where the professional conduct committee is requested by the council to consider a complaint or is in receipt of a written complaint alleging that a member is guilty of professional misconduct or professional incompetence, the committee shall:
>
> (a) review the complaint; and
>
> (b) investigate the complaint by taking any steps it considers necessary, including summoning before it the member whose conduct is the subject of the complaint or assessing the member's competence.

[68] Subsection 27(4)(h) of HIPA allows a trustee to disclose personal health information to a health professional body for the purpose of carrying out its duties pursuant to an Act with respect to regulating the profession. It provides:

> 27(4) A trustee may disclose personal health information in the custody or control of the trustee without the consent of the subject individual in the following cases:
> …
> (h) subject to subsection (5), where the disclosure is being made to a health professional body or a prescribed professional body that requires the information for the purposes of carrying out its duties pursuant to an Act with respect to regulating the profession;

[69] Subsections 24(2) and 26(2)(a) of HIPA also allow trustees to collect and use personal health information for these purposes. As such, the College is authorized to collect and use personal health information for the purpose of carrying out its duties pursuant to section 27 of *The Paramedics Act*.

[70] In this case, the College accepted the PCR numbers and other personal health information from the Informant and subsequently used this personal health information by bringing it forward to its Professional Conduct Committee. These data transactions are represented by data transaction 11 on the data flow chart. The personal health information in the Informant's complaint included PCR numbers and details of injuries and health services provided to the subject individual by the Paramedic.

[71] I note that the personal health information was de-identified at this point; however, the College was later able to re-identify the subject individual based on personal health information given as described in subsection 3(2)(a) of HIPA.

[72] While the College is authorized to collect and use personal health information for the purpose of investigating a complaint against one of its members, I have several concerns with this particular collection and use.

[73] First, the Informant had no authority to have accessed or disclosed the personal health information in question. The Informant's e-mail to the College stated "I personally have never had any problems with this paramedic because I have never worked with him, but numerous staff where(sic) telling me that they felt uncomfortable on calls with [him]." This should have raised red flags with the College.

[74] The College should have taken steps to check with the Informant to verify whether the Informant had permission to access the personal health information and to disclose on behalf of the trustee.

[75] The College submitted that its *Code of Professional Conduct* indicates that members have a legal obligation to report activity that is not ethical or legal to the College. However, I also note that the same code requires members to hold "personal information" in confidence.

[76] The Informant should have taken her concerns through proper channels before disclosing personal health information. This would have entailed raising her concerns with her employer first. The College's website advises those with concerns to take such steps. However, North East alleges that the Auditor's concerns were not brought to the attention of North East's management until after the complaint was made to the College. Only if her concerns went unaddressed should she have gone to the College. Even then, her complaint should have included only general information about her concerns. It should have been up to the investigative committee to retrieve any personal health information it requires from North East.

[77] The College's website counsels individuals on how to make a complaint about a paramedic. It states:

> When you are submitting a complaint please try to provide as much detail as possible. Information like the name of the member, the date and time of the incident being complained of, the place where the incident occurred and a detailed description of the complaint, is very helpful. If there were any witnesses to the incident, names and contact information should also be included.

[78] I recommend that the College advise its members on this website to only disclose personal health information only if it has a need-to-know and authorization from the trustee with custody or control.

[79] I also recommend that the College amend its *Code of Professional Conduct* to properly recognize personal health information and reflect paramedics' responsibilities under HIPA.

[80] As a trustee, the College also has a duty to ensure it collects accurate personal health information. Section 19 of HIPA provides:

> 19 In collecting personal health information, a trustee must take reasonable steps to ensure that the information is accurate and complete.

[81] Even though the College knew that the Informant had no direct knowledge of this personal health information, it went ahead and used the personal health information by requesting the full PCRs from the Ministry. I am not satisfied it took steps to ensure that the information is accurate and complete before using the personal health information and involving a third party.

[82] For the reasons outlined above, I am not satisfied that the College's collection and use of personal health information was appropriate in this instance.

6. Did the College have authority to disclose personal health information to the Ministry?

[83] Once the College decided to go forward with an investigation in to the Informant's complaint against the Paramedic, it decided to collect all of the PCRs in their entirety. The College approached the Ministry to ask it to provide the PCR's to them. During that process, it disclosed the PCR numbers to the Ministry, which is reflected in data transaction 12 on the data flow chart.

[84] I note that the Ministry had no responsibility for the management of this individual.

[85] The College relies on section 27 of *The Paramedics Act* which allows the investigative committee to take any steps it considers is necessary, including summoning before it the member whose conduct is the subject of the complaint or assessing the member's competence. This is supported by subsection 27(4)(l) of HIPA.

[86] I agree that obtaining more information regarding the PCRs was necessary for the committee to continue its investigation.

[87] I do not agree that disclosing the PCR numbers to a third party was best practice when there was a more appropriate option.

[88] North East should have been the point of contact for the College for the following reasons: 1) North East also had copies of the PCRs; 2) the Informant did not have direct knowledge of the events in question and the College did not know if the numbers were accurate; and 3) North East also has responsibility for supervision of the Paramedic, the Informant and other witnesses that may have direct knowledge of the events in question, while the Ministry did not. The College did not address in its submission why it did not approach North East.

[89] In response, the College said that it went to the Ministry because of concerns that North East might not comply with its request. If so, the College would have no authority to

force North East to do so. North East has indicated that the College made no attempt to contact it to request the personal health information.

[90] The College provided my office with its *Risk Management Compliance Document* which includes several policies. The *Confidential Data Policy* in this document indicates that confidential data includes personal health information, but does not define personal health information. The policy has a section entitled "Sharing Confidential Data with Third Parties" and requires a written agreement is in place before data is shared. It does not provide information on when it is appropriate to disclose personal health information. This policy is not reasonable to meet the duties imposed by section 16 of HIPA. I recommend that the College provide its policies to my office for review and feedback.

[91] I am not persuaded that the College followed best practice when it disclosed personal health information to the Ministry of Health for the purpose of collecting the PCRs.

7. Does FOIP have any application in these circumstances?

[92] As noted, the Ministry is a government institution for the purposes of FOIP.

[93] Section 25 of FOIP provides:

> 25 No government institution shall collect personal information unless the information is collected for a purpose that relates to an existing or proposed program or activity of the government institution.

[94] Subsection 24(1)(b) of FOIP states:

> 24(1) Subject to subsections (1.1) and (2), "personal information" means personal information about an identifiable individual that is recorded in any form, and includes:
>
> …
>
> (b) information that relates to the education or the criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;

[95] The fact that an individual is being investigated by a regulatory body of which he is a member would qualify as employment history and personal information pursuant to subsection 24(1)(b) of FOIP.

[96] The Paramedic in question is identifiable by the Ministry pursuant to subsection 24(1) of FOIP because his signature and paramedic number is on every one of the 10 PCRs. When the College e-mailed the Ministry requesting the PCR's it noted that it was for the purpose of addressing a complaint about a member.

[97] In its submission, the Ministry noted that it had never before received a similar request and admitted it does not have a policy on this matter – it is not an existing or proposed program or activity. As such, I must conclude that this was an unauthorized collection of the Ministry's personal information.

[98] I recommend the Ministry provide notification to the Paramedic.

8. Were the remaining data transactions authorized by HIPA?

[99] Once the College disclosed the PCR numbers to the Ministry, five further data transactions took place: the Ministry collected and used the personal health information to find the PCRs (data transaction 13); the Ministry disclosed the PCRs to the College (data transaction 14) and finally the College collected and used the PCRs for their investigation (data transaction 15).

[100] As detailed in this report, before these final five data transactions occurred, a number of unauthorized transactions occurred. To summarize:

- the Ministry did not follow section 23 of HIPA (data minimization and need-to-know principles) when it collected the 10 PCR's in their entirety;
- there was an unauthorized use of personal health information when the Auditor disclosed personal health information to the Informant;
- there was an unauthorized disclosure of personal health information when the Informant disclosed personal health information to the College;
- North East did not have reasonable safeguards in place to prevent the unauthorized use and disclosure;

- the College did not verify the accuracy of the personal health information when it collected it from the Informant who clearly did not have a need-to-know;
- the College did not follow best practises when it disclosed personal health information to a third party who did not have responsibility for managing the Paramedic;
- the Ministry made an unauthorized collection of the personal information of the Paramedic under FOIP.

[101] I do acknowledge that when the Ministry received the request, it immediately involved the Health Information and Privacy Branch. I also acknowledge that careful consideration was given by the Ministry. Under different circumstances, the final five transactions may have been authorized by subsection 27(4)(h) of HIPA However, for the reasons listed above I find these transactions were not authorized by HIPA.

[102] It also occurs to me that the subject individuals of the 10 PCRs likely have no idea that their personal health information was involved in 15 data transactions involving four different trustees. Further, nine of these transactions were unauthorized. I recommend that the College, the Ministry and North East work together to come up with a strategy to provide notification to these individuals.

[103] In response, the College said that they would not give notification to the subject individuals until the conclusion of its discipline hearing to ensure the hearing is not influenced or tainted in any way. I have already found that the College is not authorized to use the personal health information for these purposes. I recommend that the College notify the subject individuals immediately and obtain consent before proceeding to use this personal health information for these purposes.

III FINDINGS

[104] I find that HIPA applies in these circumstances.

[105] I find that the Ministry has not demonstrated that it follows the data minimization and need-to-know principles enshrined in section 23 of HIPA when it collects all of the personal health information on PCRs.

[106] I find that the Ministry has not demonstrated it has authority to use personal health information for the purposes of responding to complaints.

[107] I find there was an unauthorized use of personal health information when the Auditor shared personal health information with the Informant.

[108] I find there was an unauthorized disclosure of personal health information when the Informant disclosed personal health information to the College.

[109] I find the College did not take steps to verify the accuracy of the personal health information it collected pursuant to section 19 of HIPA and its collection and use of the personal health information was unauthorized.

[110] I find the College did not follow best practices when it disclosed personal health information to the Ministry.

[111] I find that, pursuant to section 25 of FOIP, the Ministry collected the personal information of the Paramedic without authorization.

[112] I find that the Ministry did not have authority to collect and use the PCR numbers from the College.

[113] I find the Ministry did not have authority to disclose PCRs to the College.

[114] I find the College did not have authority to collect or use the PCRs in these circumstances.

[115] I find that North East did not have adequate safeguards to prevent the unauthorized transactions.

[116] I find that the College did not have adequate safeguards to prevent the unauthorized transactions.

IV RECOMMENDATIONS

[117] I recommend the Ministry reevaluate its need to collect all personal health information on every PCR and consider changes to the PCR as discussed under issue two in this Report.

[118] I recommend that North East develop a policy and procedure respecting the use of auditing PCRs for the purpose of employee management.

[119] I recommend that North East implement all of the safeguards discussed in this report in its organization.

[120] I recommend that the College advise its members on this website to only disclose personal health information only if it has a need-to-know and authorization from the trustee with custody or control.

[121] I recommend that the College amend its *Code of Professional Conduct* to properly recognize personal health information and reflect paramedics' responsibilities under HIPA.

[122] I recommend that the College provide its policies to my office for review and feedback.

[123] I recommend the Ministry provide notification to the Paramedic regarding the unauthorized collection of personal information pursuant to FOIP.

[124] I recommend that the College, the Ministry and North East work together to come up with a strategy to provide notification to the 10 subject individuals.

[125] I recommend that the College obtain consent before proceeding to use the personal health information of the 10 affected individuals for a discipline hearing.

Dated at Regina, in the Province of Saskatchewan, this 17th day of August, 2017.

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