Office of the
Saskatchewan Information
and Privacy Commissioner

# INVESTIGATION REPORT 024-2018

## Dr. Svitlana Cheshenchuk

**August 7, 2018**

**Summary:** As a result of an investigation by the College of Physicians and Surgeons of Saskatchewan (CPSS), Dr. Svitlana Cheshenchuk admitted guilt of professional misconduct with respect to the medical record of an individual. Dr. Cheshenchuk altered the electronic record of one encounter eight times between October 20, 2014 and June 22, 2015. The Commissioner also investigated. He found that the Dr. Cheshenchuk did not have relevant policies and procedures in place. He found that Dr. Cheshenchuk did not comply with subsections 16(a), (b)(i) and (iii) or section 19 of *The Health Information Protection Act* (HIPA). He recommended that Dr. Cheshenchuk research best practices with respect to the timeliness of completing notes, making corrections to personal health information, adding late entries to personal health information and blocking access of personal health information. He recommended that Dr. Cheshenchuk create a privacy impact assessment and policies and procedures.

## I BACKGROUND

[1] On June 1, 2015, Dr. Svitlana Cheshenchuk was informed by the College of Physicians and Surgeons of Saskatchewan (CPSS) that there was a complaint against her regarding care she had given to the affected individual on October 17, 2014. The affected individual had passed away later that day and the complaint was made by the individual's family. During the course of CPSS' investigation, Dr. Cheshenchuk was charged with professional misconduct. The charges included the failure to maintain records of the affected individual that met the requirements of CPSS' bylaw 23.1 and altering the electronic record eight times between October 20, 2014 and June 22, 2015.

[2] On January 19, 2018, CPSS acknowledged that Dr. Cheshenchuk admitted guilt of professional misconduct while practicing medicine in the province of Saskatchewan in relation to her actions with the record.

[3] On February 2, 2018, my office notified Dr. Cheshenchuk that I would also be undertaking an investigation.

## II DISCUSSION OF THE ISSUES

### 1. Does HIPA apply in these circumstances?

[4] *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.

[5] Personal health information is defined in subsection 2(m) of HIPA which provides:

> 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;

[6] The original unaltered record included registration information such as name, date of birth and health services number. This qualifies as personal health information pursuant to subsection 2(m)(v) of HIPA. It also contains checked boxes that explains the physician's assessment of the individual's complaints, allergies and examination. Further, there is also some text boxes that describes the physician's assessment and diagnosis. This qualifies as personal health information because it is information with respect to the physical health of the individual, information with respect to health services provided to the individual and information that was collected in the course of providing health services to the individual. This all qualifies as personal health information pursuant to subsections 2(m)(i), (ii) and (iv)(A) of HIPA.

[7] Subsection 2(t) of HIPA defines a trustee. The relevant provisions are as follows:

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

[8] Dr. Cheshenchuk is a physician who is licensed through CPSS pursuant to *The Medical Profession Act, 1981*. Order in Council 318/2018 lists the Minister of Health as responsible for *The Medical Profession Act, 1981*. As such, Dr. Cheshenchuk qualifies as a trustee pursuant to subsection 2(t)(xii)(A) of HIPA.

[9] The personal health information must also be in the custody or control of a trustee. The record was found in the Accuro electronic medical record (EMR) of Quance East Medical Clinic where Dr. Cheshenchuk had practiced medicine and where she attended to the individual on October 17, 2014. A Saskatchewan Corporate Registry search indicates that Dr. Cheshenchuk is a fifty percent share holder in Quance East Medical Clinic Inc. Therefore, the personal health information in question was under the custody and control of Dr. Cheshenchuk.

**2. Do Dr. Cheshenchuk's actions qualify as a privacy breach?**

[10] Under HIPA, a trustee must work to maintain the integrity, accurateness and completeness of personal health information. Sections 16 and 19 of HIPA provide:

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

[11] With respect to subsections 16(a) and (b)(i), integrity refers to the condition of information being whole or complete; not modified, deleted or corrupted.

[12] CPSS' decision with respect to the complaint of the family of the affected individual noted that Dr. Cheshenchuk admitted guilt to charges of professional misconduct which related to:

- the failure to maintain the affected individual's records;
- several alterations made to the affected individual's records;
- the failure to exercise due diligence to ensure that the information in the affected individual's records accurately reflected the care provided to the affected individual; and
- the record of the encounter with the affected individual was not completed in a timely manner.

[13] In her submission to my office, Dr. Cheshenchuk noted that some of the personal health information (such as blood pressure reading) may not have been accurate when added/or

modified in the affected individuals chart after the October 17, 2014 encounter. In addition, CPSS concluded that other relevant personal health information about the affected individual's encounter with Dr. Cheshenchuk was not recorded in the EMR. This includes specifics of the encounter on October 17, 2014. By not recording all relevant information at the time of the visit, Dr. Cheshenchuk did not collect complete personal health information. Therefore, by not entering all relevant personal health information at the time of the visit, and not recording the correct personal health information, Dr. Cheshenchuk did not collect complete and accurate personal health information. She did not meet the requirements of section 19 of HIPA.

[14] Below is a timeline of the activity Dr. Cheshenchuk had with the record created with respect to the October 17, 2014 encounter.

| Date | Action |
|---|---|
| October 17, 2014 | Affected individual presents at the clinic.<br>Record of visit is created (the record).<br>Affected individual passes away later in the day. |
| October 20, 2014 | Dr. Cheshenchuk learns that the affected individual has passed away.<br>Dr. Cheshenchuk adds information in an "Assessment" field in the record. |
| October 22, 2014 | Dr. Cheshenchuk alters the new information added to "Assessment" field in the record on October 20, 2014 by adding more information. |
| February 18, 2015 | Dr. Cheshenchuk again alters the new information added to "Assessment" field in the record on October 20, 2014 twice on this day. |
| May 21, 2015 | Dr. Cheshenchuk adds new specific personal health information to "other findings" field in the record, including a blood pressure reading. Dr. Cheshenchuk changes diagnosis field. |
| June 10, 2015 | Dr. Cheshenchuk deletes some of the personal health information added on May 21, 2015 in the "Other Findings" field. She changes the diagnosis field back to what it was prior to May 21, 2015. |
| June 15, 2015 | Dr. Cheshenchuk again alters the new information added to "Assessment" field in the record on October 20, 2014. |
| June 22, 2015 | Dr. Cheshenchuk altered blood pressure reading again and checked additional boxes in the "Complaints" section. |

[15] CPSS' decision with respect to the complaint of the family of the affected individual noted that Dr. Cheshenchuk admitted guilt to charges of professional misconduct. The decision and letter to Dr. Cheshenchuk stated that:

> Honesty and integrity must be demonstrated by physicians at all times, as it is crucial to public trust and the high esteem physicians are held to by the general public.
> …
> When medical records are changed in a poorly documented manner after an adverse event, there is significant suspicion that the interaction may not have been as documented.

[16] CPSS' letter indicated that modification of a chart after seeing a patient is acceptable, but it must be done in such a manner that the original entry is still very apparent. It also noted that the reason for the modification must also be present on the chart. The Canadian Medical Protective Association (CMPA's) website, which was referenced by CPSS, states:

> It is best to document events as soon as possible following the event (contemporaneous). This is because memory about details tends to fade with time, other events may occur, and there may be disputes concerning their sequence. For example, it may later be important to know if certain symptoms or findings were present before or only after a particular caregiver's intervention.
>
> https://www.cmpa-acpm.ca/serve/docs/ela/goodpracticesguide/pages/communication/Documentation/when_to_document-e.html
>
> **Correcting the medical record**
>
> There are times when information is entered incorrectly — perhaps on the wrong patient's record by accident or perhaps due to a misunderstanding or just a "slip of the pen." Corrections can be made, but must be done properly to avoid an appearance of deliberate falsification.
>
> **On a *paper record*:**
> - Cross out incorrect information with a single line, date and initial it.
> - The original information should still be legible.
> - Write the correction and the date you write it.
> - If there have been subsequent notes, place the correction after the latest, date it, note the date of the notation being corrected and include the reason for the correction (new information, patient corrected self, etc.).

> NEVER make a correction or change an entry after learning of a complaint or legal action.
>
> **On an *electronic record*:**
> - Indicate the reason for the change.
> - Enter the correct information.
>
> An EMR should have an audit function that will indicate who made any entries or changes and when. If the EMR allows deletion, it should store and permit access to deleted text.
>
> NEVER allow others to use your password, use someone else's password, or make changes after learning of a complaint or legal action.
>
> https://www.cmpa-acpm.ca/serve/docs/ela/goodpracticesguide/pages/communication/Documentation/problems_and_pitfalls-e.html

[17] These standards should be adopted by all trustees, not just physicians who are trustees. They are supported by the *2013 Guidelines for the Protection of Health Information* by Canada's Health Informatics Association (COACH). It states:

> Healthcare organizations and providers should take reasonable steps to ensure the [personal health information] of subjects of care is as accurate and complete as necessary for the purposes for which it is to be used or disclosed. Healthcare providers must demonstrate that they use due diligence in addressing accuracy of information. Such diligence includes written policies, which should cover:
> - Documentation requirements (when to document, which tools to employ).
> - Content guidelines (objective, not subjective).
> - Timeliness of documentation (as close as possible to data collection).
> - Procedures for correcting errors and for editing (no blackouts or destruction).
> - Procedures for capturing omissions (late entries)…

[18] Dr. Cheshenchuk provided my office with a copy of the Quance East Medical Clinic Inc. privacy policies and procedures. They were put in place in May 2011 and were in place during the eight month time period in which changes were made to the record. In general, the policies and procedures cover many areas that my office would expect. This includes how to make amendments to personal health information when requested by the subject individual. However, it does not address the need to protect the integrity and accuracy of

the information pursuant to subsections 16(a), (b)(i) and (iii) of HIPA. As such, Dr. Cheshenchuk did not comply with these sections of HIPA.

**3. Did Dr. Cheshenchuk respond appropriately to the breach?**

[19] 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 Dr. Cheshenchuk 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. Plan for prevention; and
5. Write a privacy breach report.

[20] I will use these steps to assess the Dr. Cheshenchuk's response to the breach.

***Contain the Breach***

[21] 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:

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

[22] In situations where an employee of a trustee contravenes HIPA and/or privacy policies and procedures, I would expect the trustee to stop the unauthorized practice by revoking the employee's access privileges until the situation can be assessed and the employee educated, if appropriate. In this case, the trustee was a single individual and the person who contravened subsections 16(a), (b)(i) and (iii) and section 19 of HIPA. In the end, CPSS suspended Dr. Cheshenchuk's licence for one month and she was required to undergo some training. However, this occurred approximately two years after the modifications to the

record in question. This emphasizes the need of a trustee to understand their obligations under HIPA and have policies and procedures in place, especially if they are an individual.

***Notify affected individuals and/or appropriate organizations***

[23] 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.

[24] In this case, the affected individual was deceased and the family was informed through the CPSS process.

[25] Dr. Cheshenchuk did not proactively report the breach to my office.

***Investigate the breach***

[26] 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.

[27] Dr. Cheshenchuk received professional assistance in the investigation of the breach. As noted earlier, she admitted guilt in the charges made by CPSS.

[28] In her submission to my office, Dr. Cheshenchuk discussed the safeguards that were in place at the time of the breach. I have already discussed the deficient policies and procedures that were in place in the time frame in question.

[29] Another important safeguard that Dr. Cheshenchuk did have in place is an audit log in her clinic's EMR. The *2013 Guidelines for the Protection of Health Information* by Canada's Health Informatics Association (COACH) states:

> Monitoring for the detection of unauthorized information processing activities includes creating, storing and analyzing records about information transactions...
> The following security principles generally apply:
> - Confidentiality: The event records and log files should not be disclosed to unauthorized entities, since they contain information related to the communication.
> - Integrity: The event records and log files should be protected from unauthorized modification for internal or external entities.
> - Access control: Access to the event-generation sources and the resulting log files themselves should be controlled, and only authorized entities should have access privileges.
> - Traceability: Any read or write access to the log file should be traceable to be able to identify the source of an illegal action.

[30] The audit log assisted in identifying the breach.

[31] I am satisfied that Dr. Cheshenchuk's investigation was adequate. However, Dr. Cheshenchuk should have undertaken the investigation as soon as the appropriateness of her actions were called into question.

***Plan for prevention***

[32] The next 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.

[33] Dr. Cheshenchuk's submission noted that she is taking the following actions to address the privacy breach:

- blocking access to all patient records after a patient is deceased;
- completing patient notes on the day of a patient's attendance at the Clinic;
- if a late charge entry is needed, will specifically identify the note as a late entry;

- updating the Clinic's Privacy Policies in accordance with any guidance and recommendations of my office; and
- taking a medical record keeping course as directed by CPSS.

[34] With respect to the first action proposed by Dr. Cheshenchuk, it is an interesting idea, but many questions come to mind. For example, in this case, is there a difference between blocking and masking? Would the need ever arise where the personal health information of a deceased individual need to be accessed? If so, would Dr. Cheshenchuk block access from all individuals working in her clinic, including herself, or would someone who works there have the ability to unblock the information? Who would have the ability to do so? Further, if there is no need to ever access this personal health information, why would Dr. Cheshenchuk need to keep the personal health information? Would destruction of the personal health information be a more secure option? Would destruction comply with HIPA or other statutes? I recommend that Dr. Cheshenchuk research best practices regarding blocking access of personal health information of individuals and create a Privacy Impact Assessment (PIA). I recommend that Dr. Cheshenchuk submit the PIA to my office for review.

[35] I also recommend that Dr. Cheshenchuk research best practices with respect to the timeliness of completing notes, making corrections to personal health information and adding late entries to personal health information. I recommend that Dr. Cheshenchuk, develop policies and procedures on these topics that reflect best practices. She should also ensure that her staff is educated with respect to the new policies and procedures.

***Write a privacy breach report***

[36] Dr. Cheshenchuk has created a privacy breach report.

## III FINDINGS

[37] I find that Dr. Cheshenchuk did not comply with section 19 of HIPA.

[38] I find that Dr. Cheshenchuk did not comply with subsections 16(a), (b)(i) and (iii) of HIPA.

## IV RECOMMENDATIONS

[39] I recommend that Dr. Cheshenchuk research best practices regarding blocking access of personal health information of individuals and create a Privacy Impact Assessment (PIA). I recommend that Dr. Cheshenchuk submit the PIA to my office for review.

[40] I recommend that Dr. Cheshenchuk research best practices with respect to the timeliness of completing notes, making corrections to personal health information and adding late entries to personal health information. I recommend that Dr. Cheshenchuk develop policies and procedures on these topics that reflect best practices. She should also ensure that her staff is educated with respect to the new policies and procedures.

Dated at Regina, in the Province of Saskatchewan, this 7th day of August, 2018.

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