Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 080-2017

Dr. Hakan Pehlivan

September 28, 2017

Summary: A breach occurred when the office of Dr. Hakan Pehlivan disclosed the personal health information of 12 other individuals to one of his patients. Although Dr. Pehlivan did notify the 12 affected individuals of the breach, the Commissioner found that he did not follow best practices when responding to the breach. Dr. Pehlivan closed his practice and his licence was revoked during the course of the investigation. As a result, the Commissioner had no recommendations.

I BACKGROUND

[1] On April 10, 2017, an individual (the individual) contacted my office. She and her husband went to Dr. Hakan Pehlivan's office to pick up copies of the husband's personal health information. They also received personal health information of 12 other individuals among the husband's medical records. These records were in paper form.

[2] My office contacted Dr. Pehlivan by telephone on April 10, 2017 to inform him of the alleged breach and confirm his office had disclosed the personal health information. He confirmed this was an unauthorized disclosure of personal health information.

[3] My office retrieved the personal health information in question from the individual; on April 19, 2017. On April 21, 2017, my office provided notification by e-mail to Dr. Pehlivan to let him know my office would be undertaking a privacy breach investigation.

[4] On June 5, 2017, Dr Pehlivan replied to my office with a short e-mail addressing the breach. On June 13, 2017, my office notified Dr. Pehlivan of what best practices were when investigating a privacy breach and asked him specific questions relating to the breach. After several reminders, Dr. Pehlivan did not respond.

[5] On August 24, 2017, Dr. Pehlivan indicated that he had closed his practice and left the country. He said that he would provide further information about the breach as required. On August 28, 2017, my office again provided Dr. Pehlivan with advice about best practices when dealing with a privacy breach. My office asked for a response by September 11, 2017. My office did not receive one.

II DISCUSSION OF THE ISSUES

1. Does HIPA apply in these circumstances?

[6] 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.

[7] 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;

[8] The information in question appears to be medical reports written by other physicians and trustees and sent specifically to Dr. Pehlivan. This information qualifies as personal health information pursuant to subsection 2(m)(i), (ii) and (v) because it is information with respect to the physical or mental health of, health services provided to and registration information of the 12 individuals.

[9] 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

[10] At the time of the breach, Dr. Pehlivan qualified as a trustee pursuant to subsection 2(t)(xii)(A) of HIPA. The College of Physicians and Surgeons of Saskatchewan (CPSS) confirmed he was licensed pursuant to *The Medical Profession Act, 1981* from July 2009 to August 31, 2017 (with a small gap). However, the licence was revoked on August 31, 2017.

[11] The records in question were given to the individual by Dr. Pehlivan's office. Each record indicates that it was destined for Dr. Pehlivan. Therefore, I am satisfied that the personal health information was in his custody and under his control at the time of the disclosure.

2. Did Dr. Pehlivan follow best practices in his response to this privacy breach?

[12] 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. Pehlivan 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.

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

Best Practice Step 1: Contain the breach

[14] 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.

[15] My office was informed of the breach before Dr. Pehlivan was made aware. My office retrieved the personal health information from the individual and secured it until my office determined it was under Dr. Pehlivan's control and he agreed to take it back. My office did not disclose the name of the individual to Dr. Pehlivan. In communications to my office, he did not indicate if he had taken any further steps to contain the breach.

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

[16] 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.

[17] On June 5, 2017, Dr. Pehlivan reported that he notified all of the affected individuals of the breach by mail. He provided my office with a sample copy of the letter he sent to the affected individuals. He also reported that one of the individuals had passed away since the time of the breach.

[18] On August 24, 2017, Dr. Pehlivan also indicated that, in addition to written notification, he spoke with five of the affected individuals in person and some others by telephone.

[19] I am satisfied that Dr. Pehlivan notified the affected individuals.

Best Practice Step 3: Investigate the breach

[20] 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.

[21] Dr. Pehlivan's e-mail of June 5, 2017 indicated that he had completed his investigation. However, it indicated that he was "not sure" if the package received by the individual was received as one file from Dr. Pehlivan's previous office or if they were attached together at his new office by his employee.

[22] My office specifically asked Dr. Pehlivan to explain the circumstances regarding the transfer of the personal health information from his old office to his new office. We asked if the files were sent to his new office just to respond to an access request or if the files were transferred to him for the purpose of the move. Dr. Pehlivan did not address these questions.

[23] Section 16 of HIPA 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.

[24] Dr. Pehlivan's communication did not address any safeguards in place at the time of the privacy breach. He did not say if there were policies or procedures in place regarding giving individuals access to their own personal health information. He did not indicate if there were any privacy policies or procedures in place. He did not indicate if the employee who disclosed the personal health information had privacy training. These are all safeguards that are required by section 16 of HIPA. Further, if any safeguards were in place at the time of the breach, he did not investigate if they were used or why they were not able to prevent the breach.

[25] I am not satisfied that Dr. Pehlivan thoroughly investigated this matter. He did not identify the root cause or any safeguards that may have been in place at the time of the breach.

Best Practice Step 4: Prevent future breaches

[26] 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.

[27] In his communications to my office, Dr. Pehlivan indicated that some of the measures he put in place included being "extra careful printing large files" and "checking to each page" before releasing personal health information to individuals. He did not indicate whether this would be communicated to employees through formal written policies and procedures.

[28] Further, it is difficult to put effective measures in place when the root cause of the breach was unknown. Perhaps lack of training and written policies and procedures were to blame. However, perhaps those safeguards were in place and the breach was the cause of a different root cause. This might include poor filing practices or a lack of a clear understanding of custody and control of personal health information between Dr. Pehlivan's new office and old office.

[29] The difficulty my office is facing is the lack of communication with Dr. Pehlivan. As noted, CPSS revoked Dr. Pehlivan's licence on August 31, 2017. Further, he has left the country and several organizations that my office has spoken to report he is also unresponsive to their efforts to communicate. Without more knowledge about the circumstances at the time of the breach, I am unable to make informed recommendations. Additionally, as Dr. Pehlivan no longer practices, it does not make sense to make recommendations regarding his practice. Therefore, I have no recommendations at this time.

[30] I will be forwarding this report to CPSS. In the event that Dr. Pehlivan reapplies for a medical licence in Saskatchewan, I would ask CPSS to ask Dr. Pehlivan to contact my office.

Best Practice Step 5: Prepare a privacy breach report

[31] Dr. Pehlivan did not prepare a privacy breach report.

III FINDING

[32] I find that Dr. Pehlivan did not follow best practices in responding to this privacy breach.

IV RECOMMENDATION

[33] I have no recommendations at this time.

Dated at Regina, in the Province of Saskatchewan, this 28th day of September, 2017.

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