



INVESTIGATION REPORT 195-2016

Dr. Jacobus DeWitt

September 22, 2016

Summary:

The Complainant alleged that an envelope containing her personal health information that was addressed to her at her husband's office was opened by Dr. DeWitt's receptionist. Dr. DeWitt and the Complainant's husband share office space. The Commissioner found that Dr. DeWitt could have taken better steps to respond to the breach. He recommended some improvements to Dr. DeWitt's procedures. He also recommended that the Complainant have her personal health information sent to her home address.

I BACKGROUND

- [1] My office received a complaint from the wife of a physician that shared office space with Dr. DeWitt. The Complainant also worked in her husband's office. She alleged that, on May 25, 2016, Dr. DeWitt's Office Manager opened an envelope addressed to her which contained her personal health information. She also alleged that the Office Manager then handed it to the Complainant's husband's receptionist who placed the letter face up on the reception desk.
- [2] On July 9, 2016, the Complainant wrote a letter to Dr. DeWitt raising her concerns. Dr. DeWitt replied in writing on July 28, 2016. The Complainant was unsatisfied with his response and asked my office to investigate.
- [3] On August 12, 2016, my office notified the Complainant and Dr. DeWitt of our intention to conduct an investigation.

[4] I note that the Complainant has reported that the relationship between herself, her husband and Dr. DeWitt is a contentious one.

II DISCUSSION OF THE ISSUES

1. Does HIPA apply in these circumstances?

[5] *The Health Information Protection Act* (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 if the personal health information is 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 Complainant has advised me that the document in the envelope opened by Dr. DeWitt’s Office Manager was the result of a test performed by the Saskatchewan Cancer

Agency. It also contained registration information. This qualifies as personal health information pursuant to subsection 2(m)(i), (ii) and (v) of HIPA.

[8] Dr. DeWitt qualifies as a trustee pursuant to subsection 2(t)(xiii)(A) of HIPA.

[9] My office has found that a trustee has custody of personal health information when it has physical possession. As soon as the envelope was delivered to Dr. DeWitt's office and opened, he had custody.

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

2. Did Dr. DeWitt follow best practices in its response to this privacy breach?

[11] 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. DeWitt took the privacy breach seriously and appropriately addressed it. My office's resource, *IPC Guide to HIPA*, recommends four 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; and
4. Plan for prevention.

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

Best Practice Step 1: Contain the breach

[13] 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.

[14] In this case, Dr. DeWitt's Office Manager took the personal health information to the Complainant's husband's receptionist as soon as the mistake was realized. The Office Manager informed the Complainant's husband's receptionist of the error at that time.

[15] I question why Dr. DeWitt's Office Manager gave the Complainant's personal health information to her husband's receptionist. The Code of Ethics for physicians instructs that physicians should only treat family members for minor or emergency services when another physician is not readily available. As such, I am not aware that the Complainant's husband had a need-to-know his wife's personal health information pursuant to HIPA. Further, Dr. De Witt did not indicate that he had obtained consent from the Complainant to disclose personal health information to her husband as a trustee pursuant to subsection 27(1) of HIPA. In the future, if misdirected mail intended for an individual is received by Dr. DeWitt's office the personal health information should be sent directly to the individual or back to the sender.

[16] The Complainant and her husband also have a role to play in this situation. Her personal health information was sent to her husband's place of business and not her home address. Personal health information received at her husband's place of work might be subject to HIPA. As the Complainant's husband does not have a physician-patient relationship with her, he should not be collecting her personal health information. I recommend that the Complainant ensure all her personal health information be sent directly to her home address. Especially given the contentious relationship that exists in the physical space occupied by the two physicians.

[17] The Complainant was also concerned that Dr. DeWitt's Office Manager handed the personal health information to the Complainant's husband's receptionist who then left it face up on the reception desk. It would have been better if Dr. DeWitt's Office Manager had kept the personal health information protected by putting it back in the envelope

before forwarding it to the correct recipient. However, Dr. DeWitt pointed out that he had no control over what occurred after custody was transferred to another trustee. I encourage the Complainant's husband to keep unattended personal health information in a restricted area.

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

[18] 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.

[19] Dr. DeWitt indicated that his Office Manager notified the Complainant's receptionist of the breach. Again, the individual in question was not notified in this case. Instead, someone without a need-to-know was notified. I recommend that, in the future, Dr. DeWitt's staff or Dr. DeWitt directly notify the affected individual.

[20] I note that since the Complainant raised her concerns with Dr. DeWitt, he has provided her with a letter explaining the situation and an apology.

Best Practice Step 3: Investigate the breach

[21] 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. 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.

[22] Upon review of Dr. DeWitt's response to me, it is clear that he has reviewed his office's mail procedures and interviewed his Office Manager who was involved in the breach. His response outlines all of the steps he has taken in response to the breach.

[23] In his response to my office, Dr. DeWitt explained the procedure that was in place at the time of the breach was as follows:

1. Canada Post would deliver a bundle of mail for all four physicians that share the same office space.
2. A receptionist of anyone of the four physicians who has a moment will sort the bundle of unopened mail into piles for each recipient and deliver it to the appropriate receptionist.
3. Dr. DeWitt's receptionist will then sort through his pile and remove any envelopes marked "personal" or "confidential" and place them on Dr. DeWitt's desk to be opened by him directly.
4. Then the receptionist will open the rest of the mail and take appropriate action.

[24] He reports that the Complainant's personal health information was placed in the pile for Dr. DeWitt. His office manager simply opened the envelope without checking. He ascertained that the envelope was not marked personal or confidential.

[25] I am satisfied that he has taken reasonable steps to investigate this breach and ascertain all of the relevant facts.

Best Practice Step 4: Plan for prevention

[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] Dr. DeWitt informed my office that, in response to the breach, his office has added a step to the mail procedures. The receptionist will now check all of the envelopes that have been directed to Dr. DeWitt to ensure that they are intended for Dr. DeWitt. He has also created a procedure on how to deal with a misdirected unopened piece of mail.

[28] Dr. DeWitt also indicated that his office has adopted the following procedure if misdirected mail is opened in the future:

If, notwithstanding the above steps, a piece of mail is opened that was not intended for our office, it will be placed in an envelope and addressed to the intended recipient, with an explanatory note regarding the error. I am to be made aware of such an error occurring right away.

[29] Receiving a misdirected piece of mail is similar to receiving a misdirected fax. Page 154 of the *IPC Guide to HIPA* explains the steps that are necessary when a misdirected fax has occurred. I recommend that Dr. DeWitt include the steps described on this page to his procedure for dealing with misdirected mail. I note that it is necessary to notify the affected individual when an envelope is opened by mistake because the receiving trustee actions are involved in the breach.

[30] Dr. DeWitt has also indicated that he is trying to set up a meeting with the other physicians who share the physical space to discuss the handling of mail in the physical space. I recommend the physicians inquire with Canada Post if separate mail drops by the mail carrier are possible or even consider having mail delivered to separate post office boxes.

III FINDINGS

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

[32] I find that Dr. DeWitt did not follow best practices when responding to the breach.

IV RECOMMENDATIONS

[33] I recommend that the physicians look into getting separate mail drops or separate post office boxes from Canada Post.

[34] I recommend Dr. DeWitt make improvements to the following procedures:

- notifying affected individuals;
- receiving misdirected mail.

[35] I recommend that the husband of the Complainant ensure that he only collect the personal health information of individuals he has a physician-patient relationship with and that the personal health information of the Complainant is sent to their home address.

Dated at Regina, in the Province of Saskatchewan, this 22nd day of September, 2016.

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