Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 066-2017

MD Ambulance

June 13, 2017

Summary: An email with an attachment containing personal health information was erroneously sent by MD Ambulance. The Information and Privacy Commissioner (IPC) found that MD Ambulance took some steps to respond to the privacy breach but not all. The IPC made a number of recommendations including MD Ambulance instructing unintended recipients of errant emails to not further distribute or download the email and attachments and to delete the errant emails and their attachments.

I BACKGROUND

[1] At 2:30 p.m. on March 30, 2017, MD Ambulance sent an email with an attachment to the Credit Bureau of Saskatchewan and another company (Company X). The email requested that a report similar to the report attached to the email be sent to MD Ambulance. The report attached to the email is a list of individuals who are indebted to MD Ambulance. It includes first names, last names, amount owing, account numbers, and the Credit Bureau of Saskatchewan's recommendations not to pursue the debt and the reason for the recommendations.

[2] The email was not intended for Company X. At 7:29 a.m. on March 31, 2017, the VP Program Development of Company X responded to the email asking MD Ambulance if the email and attachment was sent to Company X in error. According to MD Ambulance, it confirmed with the VP Program Development of Company X it was an error. It also asked Company X to delete the email.

[3] At 7:32 a.m. on the same day, another Company X employee forwarded the email to my office. He advised my office that after he forwarded the email, he had immediately deleted the email.

[4] On April 7, 2017, my office notified MD Ambulance it would be undertaking an investigation.

II DISCUSSION OF THE ISSUES

[5] *The Health Information Protection Act* (HIPA) is engaged when three elements are present: 1) a trustee, 2) personal health information, and 3) the trustee must have custody or control over the personal health information.

[6] First, the operator of MD Ambulance (which was sold to Medavie EMS) qualifies as a trustee as defined by subsection 2(t)(vii) of HIPA.

[7] Second, the information contained in the report qualifies as personal health information as defined by subsection 2(m)(ii) of HIPA, which provides:

> 2(m) "personal health information" means, with respect to an individual, whether living or deceased:
>
> ...
>
> (ii) information with respect to any health service provided to the individual;
>
> …
>
> (v) registration information;

[8] Third, MD Ambulance has custody and control over the personal health information. This is demonstrated by the fact that MD Ambulance was the one who sent the errant email with the report containing personal health information of its patients attached.

[9] I find that HIPA is engaged.

2. Was there a privacy breach?

[10] A privacy breach occurs when personal health information is not collected, used, and/or disclosed in accordance with HIPA. A privacy breach can also occur when trustees do not have sufficient safeguards in accordance with section 16 of HIPA.

[11] In this case, personal health information was inadvertently disclosed to Company X. HIPA does not authorize such a disclosure. Therefore, I find a privacy breach has occurred.

3. Did MD Ambulance respond appropriately to the privacy breach?

[12] My office recommends that trustees take the following five steps when responding to a privacy breach:

- Contain the breach,
- Notify affected individuals,
- Investigate the breach,
- Prevent future breaches, and
- Write a privacy breach report.

[13] I will consider each of these steps to determine if MD Ambulance adequately responded to the privacy breach.

Contain the breach

[14] The first step in responding to a privacy breach is containing the breach, which means to recover the personal health information or to stop the unauthorized practice when the trustee learns of the breach.

[15] In its internal investigation report, MD Ambulance learned of the breach when the VP Program Development of Company X emailed it to ask if the email it had sent was an error. MD Ambulance said "Given that the gentleman responding was a VP, [MD Ambulance] felt that the breach was contained."

[16] As noted in the background, MD Ambulance had asked Company X to delete the email. In addition, it should have also instructed the VP Program Development of Company X: 1) to not download or distribute the attachment, and 2) to send an email to MD Ambulance confirming he has followed the instructions.

[17] I find that MD Ambulance did not take some but not all appropriate steps to contain the breach.

[18] MD Ambulance provided my office with a copy of its *Confidentiality Policy*, which provides:

> All employees, or those contracted by MEDAVIE HEALTH SERVICES or affiliates must:
>
> ...
>
> Identify confidential information when sending emails or fax transmissions and to provide direction to the recipient if they receive a transmission in error.

[19] I note that in the emails exchanged between my office and MD Ambulance, MD Ambulance's emails include a boiler plate confidentiality notice. While this is good, I recommend that MD Ambulance actively instruct unintended recipients of errant emails to not further distribute or download the email and any attachments and to delete the errant emails and their attachments.

[20] In this case, Company X forwarded the errant email and attachment to my office. Therefore, my office followed up with Company X and confirmed that the email and the attachment were deleted from its inbox and the trash folder. It also deleted the email from its sent folder. It also confirmed that it only forwarded the email and attachment to my office.

Notify affected individuals

[21] Notifying an individual that their personal health information has been inappropriately disclosed 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 disclosure. Unless there is a compelling reason not to, trustees should always notify affected individuals.

[22] In this case, MD Ambulance did not notify any affected individuals. The three reasons why MD Ambulance did not notify the affected individuals are 1) the addresses MD Ambulance has on file for the individuals are invalid, 2) Company X did not further distribute the report, and 3) the data in the attachment is already in the public domain.

[23] There are certainly circumstances in which notifying affected individuals could potentially cause another privacy breach. In this case, I note that in the report that was attached to the errant email listed the reason for some debts not being collected is because the individual could not be located. If MD Ambulance does not have the correct addresses for individuals, then MD Ambulance cannot be confident that sending notification letters to the affected individual will reach the intended recipients.

[24] There are other methods to notify affected individuals. Since there are 197 affected individuals, MD Ambulance can consider posting a notice of the breach in a local but widely-distributed newspaper and/or on its website. The notice can include a description of the breach, types of information that were involved, what MD Ambulance has done to manage the breach, and the steps individuals can take to protect themselves. The notice should also include the contact information at MD Ambulance that individuals may contact so that individuals can find out if they were affected. If affected individuals contact MD Ambulance, they should be given the contact information of my office if the affected individuals wish to submit a complaint to my office as well.

[25] I find that MD Ambulance has not taken steps to notify affected individuals.

Investigate the breach

[26] The next step in responding to a privacy breach is to investigate what caused the breach. In this case, it appears that the errant email was due to auto-complete of email addresses feature in MD Ambulance's email application, Microsoft Outlook. Further, Company X's email address had been automatically added to the MD Ambulance employee's

"suggested contacts" list in Outlook. Company X was a part of the MD Ambulance employee's suggested contacts list. Therefore, Company X's email address was easily selected as a recipient of the email.

[27] Since MD Ambulance's investigation and its steps to prevent future breaches are inextricably linked, I will proceed to the next section of the five steps to manage a breach before making a finding.

Prevent future breaches

[28] The most important part of responding to a privacy breach is to implement measures to prevent future breaches from occurring. Through this process, a trustee should determine what steps can be taken to prevent a similar privacy breach.

[29] The MD Ambulance employee who had sent the email 1) disabled the auto-complete of email addresses feature on her Microsoft Outlook, 2) deleted the autocomplete list of emails, and 3) disabled the automatic addition of addresses to the "suggested contacts" list in her Microsoft Outlook. In effect, these changes will require that the sender must deliberately select the recipient from the contacts list or he/she must type the email address in full.

[30] MD Ambulance is also working on corporate-wide policies so other staff do not accidentally send errant emails as well.

[31] MD Ambulance also indicated that it has ordered additional Portable Document Format (PDF) writer licenses so that passwords can be added to any PDF files that need to be emailed.

[32] I find that the measures the MD Ambulance employee took as described in paragraph [29] to be appropriate. I recommend that MD Ambulance employees who have access to personal health information to do the same.

[33] I also find that MD Ambulance requiring passwords on PDF files being sent through email to be appropriate. Strong passwords provide an additional layer of protection. If the PDF files contain personal health information, or any identifiable information, then I recommend MD Ambulance require employees to set a strong password for PDF files before sending them. I also recommend MD Ambulance train staff to communicate to recipients so that passwords are not easily compromised. For example, if MD Ambulance is emailing a password protected document, then it should communicate the password in a method other than email.

Write a privacy breach report

[34] The final step in responding to a privacy breach is to formalize what was discovered through the previous four steps by preparing a privacy breach report. MD Ambulance used my office's resource *Privacy Breach Internal Investigation Report Guide for Public Bodies* to assist it in its investigation of the privacy breach. It provided my office with a copy of its findings of its internal investigation. Therefore, I find that MD Ambulance completed the final step in responding to a privacy breach.

III FINDINGS

[35] I find that HIPA is engaged.

[36] I find a privacy breach has occurred.

[37] I find that MD Ambulance took some but not all appropriate steps to contain the breach.

[38] I find that MD Ambulance has not taken steps to notify affected individuals.

[39] I find that the measures the MD Ambulance employee took as described in paragraph [29] to be appropriate.

[40] I find that MD Ambulance requiring passwords on PDF files being sent through email to be appropriate.

[41] I find that MD Ambulance completed the final step of responding to a privacy breach, writing a privacy breach report, appropriately.

V RECOMMENDATIONS

[42] I recommend that MD Ambulance promptly instruct unintended recipients of errant emails to not further distribute or download the email and any attachments and to delete the errant emails and their attachments.

[43] I recommend that MD Ambulance post a notice of the breach in a widely distributed local newspaper and/or its website, as described in paragraph [24].

[44] I recommend that MD Ambulance employees who require access to personal health information to do the same as the MD Ambulance described in paragraph [29].

[45] I recommend MD Ambulance require employees to set a strong password for PDF files containing personal health information before sending them.

[46] I recommend MD Ambulance train staff to communicate to recipients so that passwords are not easily compromised.

Dated at Regina, in the Province of Saskatchewan, this 13th day of June, 2017.

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