Office of the
Saskatchewan Information
and Privacy Commissioner

# Saskatchewan IPC finds ransomware attack results in one of the largest privacy breaches in this province involving citizens' most sensitive data

*January 8, 2021*

An investigation by the Information and Privacy Commissioner of Saskatchewan has found that eHealth Saskatchewan (eHealth), the Saskatchewan Health Authority (SHA) and the Ministry of Health (Health) were the victims of a ransomware attack in late December 2019 and early January 2020, resulting in one of the largest privacy breaches in this province.

On December 20, 2019, an SHA employee opened an infected Microsoft Word document from their personal email account on their personal device while the personal device was being charged by a USB cord on their SHA workstation. The infected Microsoft Word document triggered the execution of ransomware on the workstation and a multi-phase exploit took place between December 20, 2019 and January 5, 2020. This ultimately led to a Ryuk ransomware attack on January 5, 2020, where the attackers made a ransomware demand. The attack affected fileshares with eHealth, the SHA and Health due to the shared infrastructure on which the fileshares reside.

On January 21, 2020, eHealth discovered that files were disclosed to malicious internet protocol (IP) addresses in Germany and the Netherlands. In total, approximately 40 gigabytes of encrypted data was extracted.

Through its investigation, eHealth advised my office that the affected servers contained approximately 50 million files across eHealth, the SHA and Health. eHealth conducted a metadata scan of those 50 million files and identified that approximately 5.5 million of those files may contain personal information and personal health information. eHealth developed a tool to scan the 5.5 million files and that tool identified a total of 547,145 files that potentially contain personal information and/or personal health information.

As there were a minimum of 547,145 files containing personal information and/or personal health information exposed to the ransomware (possibly more depending upon the accuracy of the tool developed by eHealth), the Commissioner concluded that personal information and personal health information of citizens of Saskatchewan was either exposed to the malware or maliciously stolen from eHealth, the SHA and Health.

Through the Commissioner's investigation, it was discovered that there were three critical opportunities – two by eHealth and one by the SHA employee - where the ransomware may have been detected at an earlier stage. Had these opportunities not have been missed, eHealth may have been able to detect the ransomware, shut down its systems and stop the extraction of data.

"eHealth is charged with collecting, storing and protecting the most sensitive health data in our province," says Information and Privacy Commissioner Ron Kruzeniski. "Each of us has personal health information in eHealth's systems. It is absolutely reasonable that each citizen demand the very highest level of security on our health information. To accept less is irresponsible."

The Commissioner found that eHealth failed in fully investigating the two early threat occurrences which may have prevented the malicious extraction of data that followed. He also determined that eHealth did not sufficiently provide notification and that the SHA and Health failed in their notification efforts due to the excessive delay in providing notification. Furthermore, the Commissioner found that the SHA did not provide the employee at the heart of the incident with training on its Acceptable Use of IT [Information Technology] Assets policy.

"Because we are dealing with the most sensitive personal health information, every person who has access to this information needs to be trained, retrained and trained again as to the things they can do and especially the things they cannot do," says Information and Privacy Commissioner Ron Kruzeniski. "This incident reveals the tremendous cost of one employee doing something and other employees failing to follow up rigorously on the warnings given."

The Commissioner made a number of recommendations, including:

- that eHealth undertake a comprehensive review of its security protocols to include an in-depth investigation when early signs of suspicious activity are detected;
- that the SHA and Health take immediate steps to provide mass notification including media releases, newspaper notices, website notices and social media alerts;
- that eHealth, the SHA and Health work together and provide identity theft protection, including credit monitoring, to affected individuals for a minimum of five years from the date an affected individual's information is discovered on the dark web or to any concerned citizen who requests this protection;
- that eHealth review whether it should have IT security staff in place 24 hours a day, seven days a week to actively monitor and investigate potential threats;
- that all eHealth and eHealth partners be required to complete cyber security and privacy refresher training on an annual basis; and
- that the Minister of Health immediately commence an independent governance, management and program review of eHealth based upon the concerns put forward by SaskTel, the Provincial Auditor and this Report.

The Commissioner recognizes that organizations are under continued threat of cyber security attacks. Therefore, the organizations that hold the citizens most sensitive data must strive to have the best protected systems with the most thoroughly trained employees to mitigate the risks of these attacks happening.

The Commissioner acknowledges that, "eHealth, the SHA and Health have begun to take the necessary steps to ensure they are protecting the personal information and personal health information of the citizens of this province."

### Related Documents

Investigation Report 009-2020, 053-2020, 224-2020

Statement from the Office of the Information and Privacy Commissioner of Saskatchewan on eHealth Saskatchewan Potential Privacy Breach – January 16, 2020

### Media Contact

Kara Philip (Manager of Communication)
kphilip@oipc.sk.ca
306-798-2260