HEADWATERS Health Care Centre

Cyber Incident Update

FREQUENTLY ASKED QUESTIONS

When was this incident discovered?
On November 25, 2021, Headwaters discovered that our information technology (IT) system had been subjected to unauthorized access by cyber criminals.

Who or what accessed Headwaters Health Care Centre's system?
A third-party group accessed the IT system.

How did the person or group gain access to the system?
Access was gained through a phishing email.

Did the cyber criminals steal data?
The cyber criminals took random collection of files stored on our system. They have communicated that the data they accessed has been deleted. We have no reason to believe that the cyber criminals held on to the data or misused it in any way.

Was there ransom? Did you pay it?
This is not a question we can answer for security reasons. The cyber criminals have communicated that the data they accessed has been deleted. We have no reason to believe that the cyber criminals held on to the data or misused it in any way.

How many people were affected?
The incident affected a large number of patients, staff, former staff and donors, and these groups overlap. Most individuals were affected in a manner that did not warrant the extension of credit monitoring services.

What is Headwaters Health Care Centre doing in response to this incident?
What Headwaters has been doing to protect us in the future includes putting in place various controls such as multifactor authentication to all external connections to the network, purchased a KnowBe4 phishing simulation tool and hardened our firewall rules, among other actions.

How do I know if my information has been affected?
Over the coming days, people who have been directly affected will individually notified.

What is Headwaters Health Care Centre doing to prevent future attacks on its information technology system?
Following the incident, we implemented various additional controls such as multifactor authentication to all external connections to the network, procured a KnowBe4 phishing simulation tool, implemented a behaviour-based endpoint detection and response tool and hardened our firewall rules, among other actions.

Is this incident related to any others in our province or beyond?
We do not know.

Can we have a copy of the hospital's forensic report?
The advice of the hospital's experts is confidential and privileged, though we are committed to being open about the facts. If you have questions, please let us know by contacting the Office of the Regional Privacy Officer, privacy@headwatershealth.ca or by phone at (519) 307 0984.

Who do I contact if I have questions?
You can contact the office of the Chief Privacy Officer. They can be reached at privacy@headwatershealth.ca or by phone at (519) 307 0984.

I am a member of the media, who can I connect with about this incident?
You can email info@headwatershealth.ca

If I do not feel satisfied with Headwaters Health Care Centre's response to this privacy incident, where do I go for help?
Patients can reach out to the Information and Privacy Commissioner of Ontario at www.ipc.on.ca Staff and physicians should reach out to their union or workplace representatives.

Am I at risk?
We don't believe so. We have provided a two-year credit monitoring service to those whose key identifiers (e.g. social insurance numbers) were exposed out of an abundance of caution. Otherwise, we are encouraging everyone to be as vigilant as always regarding the risk of identity fraud.

Where can I learn more about how to protect myself?
Visit Service Canada's identity theft resources or the Canadian Anti-Fraud Centre for more information.

Will the hospital compensate me for this?
Generally, no, but if you if you feel something has happened to you because of this incident you may write us at privacy@headwatershealth.ca or call (519) 307 0984 to explain why and we will consider your situation.

Will you provide me with credit monitoring?
We are providing two-years of credit monitoring to those whose key identifiers (e.g. social insurance numbers) were exposed out of an abundance of caution. If you are affected in this way, you will receive a notice and a credit monitoring offer.

I stored personal files on my work computer. Is it at risk?
In identifying those affected, we did not look specifically for these types of files. However, we may have identified you as affected, nonetheless. For example, we looked for social insurance numbers in the stolen data, so if you stored your tax documents on the work system and those documents were taken, we likely discovered this and will notify you. Going forward, we recommend against storing personal files on the hospital's system.