

Cyber Incident FAQs

November 10, 2023

The following are frequently asked questions regarding the cyber incident based on previous updates.

What happened?

Bluewater Health, Chatham-Kent Health Alliance, Erie Shores HealthCare, Hôtel-Dieu Grace Healthcare and Windsor Regional Hospital, and our shared service provider TransForm Shared Service Organization, can confirm that we are victims of a ransomware attack. We did not pay a ransom and we are aware that data connected to the cyber incident has been published.

We condemn the actions of cyber criminals, in the healthcare sector and elsewhere, in our communities and around the world. We understand the concern this incident has raised within our communities, including patients and our employees and professional staff, and we deeply apologize.

We continue to work to strengthen our systems to prevent these types of incidents – which have become all too common for organizations across Canada and the globe.

When did it happen?

We are still investigating but first became aware of system disruption on October 23, 2023.

How did this happen?

We are continuing to investigate. Additional information can be found:

- [Update On Cyber Attacks at Regional Hospitals](#) - November 9, 2023
 - [Cyber Security Update](#) - November 6, 2023
-

When will systems be back up?

We can confirm that the restoration process is on track. While it will still take some time before all affected critical systems are completely online, our teams are working around the clock to ensure the process is progressing as quickly and safely as possible. We are also working with leads at each hospital for a seamless return to service.

This restoration is expected to be complete by mid-December. Delays will be reduced for patients once digital charting is restored. Please note that some patients and families may still experience diagnostic and/or treatment delays while we work to restore all systems. Clinical applications will be coming back online one by one or in clusters as we approach mid December 2023.

For more information on the restoration process, please see the latest update here:

- [Update On Cyber Attacks at Regional Hospitals](#) - November 9, 2023
- [Cyber Security Update](#) - November 6, 2023

A patient cybersecurity hotline has been established. For inquiries please call: **519-437-6212** (8 am to 11 pm Monday through Friday).

Was any data accessed?

Working with leading cybersecurity experts, we have determined through our investigation that, unfortunately, certain patient, employee and professional staff data has been taken. We have also become aware that data connected to the cyber incident has been published.

Our investigation has shown this attack did not involve the theft of databases linked to the following functions:

- Payroll and banking information
- Physician Credentialing
- Foundation and Donors
- Accounts Payable
- Electronic Health Record for all institutions other than Bluewater Health

We are doing a thorough investigation (called an e-discovery) to determine the extent of the information that was affected in this ransomware attack. We will promptly notify any individual directly if the investigation indicates that their information was impacted.

Please see the latest update on the data impacted:

- [Update On Cyber Attacks at Regional Hospitals](#) - November 9, 2023
 - [Cyber Security Update](#) - November 6, 2023
-

Were you hit by a ransomware attack? Did you pay a ransom?

We can confirm it was a ransomware attack. Our leaders, on advice by our experts that we could not verify claims by the attacker, decided we would not yield to their ransom demands. We are aligned in this position with the 50 members of the International Counter Ransomware Initiative (CRI), including Canada, who have recently pledged to never pay ransom to cybercriminals.

What patient data was impacted?

All hospitals have some degree of patient and employee information affected.

Please see the latest update on the data impacted:

- [Update On Cyber Attacks at Regional Hospitals](#) - November 9, 2023
 - [Cyber Security Update](#) - November 6, 2023
-

What are you doing to protect employees and professional staff?

We have made the decision to provide free credit monitoring and identify theft protection to all employees and professional staff out of an abundance of caution. We strongly encourage each employee and professional staff member to take advantage of this offering. You don't have to pay for it, and it can be instrumental in identifying any potentially fraudulent activity.

A patient cybersecurity hotline has also been established. For inquiries please call: 519-437-6212 (8 am to 11 pm Monday through Friday). Staff questions can be directed to their HR teams.

What are you doing to protect patients?

We will directly notify all those whose SIN was stolen, and they will be provided with two years of complimentary credit monitoring.

Have the police/local authorities been notified?

All relevant authorities have been notified including local police departments, Ontario Provincial Police, INTERPOL and FBI – and we have notified all relevant regulatory organizations including the Ontario Information and Privacy Commissioner.

What are you doing to prevent this from happening again?

We are working with cybersecurity experts who are helping us safely restore our IT services, investigate what happened, who is impacted and what information was affected. They are also providing guidance on further strengthening our systems.

What should I do to protect myself if I have concerns about this?

We encourage you to be vigilant and report any suspicious activity to the appropriate authorities. Tips and resources for protecting your identity are available at: https://www.priv.gc.ca/en/privacy-topics/identities/identity-theft/guide_idt/

A patient cybersecurity hotline has been established. For inquiries please call: **519-437-6212** (8 am to 11 pm Monday through Friday). Staff questions can be directed to your respective HR teams.

Bluewater Health seems to have been impacted the most – especially when it comes to patient records. Why is that?

The attackers targeted a Bluewater Health patient database.

For more information on how Bluewater Health is impacted, please see the latest update:

- [Update On Cyber Attacks at Regional Hospitals](#) - November 9, 2023
-

Which systems were impacted?

Through our investigation we know that all our clinical and non-clinical systems were impacted as they are reliant on a safe secure network. Our experts have advised us that the safest route is to rebuild the network.

What is the impact on our hospitals and frontline healthcare workers?

At this time, due to the current impact on systems, physicians may not have access to:

- Past patient records or medical history
- Patients' current medication list
- Report from other clinicians involved in care
- Pre-admission workups

While some of our systems are functional, they are slower than usual and require extra time. This affects access to labs and diagnostic imaging.

To ensure safe care, some physicians will have to cancel procedures if, in the absence of important information, they feel it is unsafe to proceed. If this is required, physicians will do their very best to reschedule as quickly as possible.

Patients also need to bring their health card to the hospital when seeking care. If patients do not need emergency care, we ask that they please attend their primary care provider or local clinic.

We want to emphasize to our patients that our physicians and frontline staff are under greater than normal stress due to these unusual circumstances, and they are responding with incredible resolve. We ask the public for their understanding during this time. This has been a challenging situation for employees, professional staff, patients and families, and we thank our community and system partners for their ongoing patience and support.

Can patients and families continue to expect delays in their care?

Some patients and families may still experience diagnostic and/or treatment delays while we work to restore all systems.

Have you reported to the Ontario Information and Privacy Commissioner (the IPC)?

These breaches have been reported to the IPC and investigation files have been opened. While you are entitled to file a complaint, the IPC has advised that it is not necessary as they are already investigating the matter. You can visit the IPC's website at www.ipc.on.ca.
