

MEDIA RELEASE

November 8, 2023
For Immediate Release

UPDATE ON CYBER ATTACKS AT REGIONAL HOSPITALS

Update on Cyber-attack: Impact and Recovery – November 8, 2023

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 were recently the 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.

The following is an update on the recovery process and important information on the limitations at our hospitals as a result of this cyber-attack (this has been shared internally to staff):

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.

Recovery Process

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.

The recovery process is happening in five phases:

1. Containment: Contain the cyber attack. ****COMPLETE****
2. Identification: Identify the cause of the cyber attack through a forensic investigation. ****ONGOING****
3. Remediation: Strengthen and add additional protections to the network. ****ONGOING****
4. Restoration: Bring back applications and systems, based on clinical priority. ****ONGOING****
5. Monitoring: Continue monitoring of traffic into and out of the network. ****ONGOING****

We can confirm that the restoration process (Phase 4) 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.

After discovering the cyber-attack, we immediately began the process to restore digital patient charting.

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.

The investigation into the incident is also in progress to determine the specific individuals whose data may have been taken, and this is expected to take a number of months.

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 respective HR teams.