# MEDIA RELEASE

November 6, 2023
For Immediate Release

# UPDATE ON CYBER ATTACKS AT REGIONAL HOSPITALS

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.

## Making Progress

We have made progress in evaluating the affected data and can share some preliminary conclusions.
This attack did not involve the theft of databases linked to the following functions:

- Employee Payroll
- Accounts Payable (i.e. vendor payments or payments to professional staff)
- Electronic Health Record for all institutions other than Bluewater Health
- Donor information

The attackers targeted a Bluewater Health patient database report. They also were able to steal data from an operations file server that housed a segmented employee shared drive used by all our hospitals. The shared drive data included patient and employee information of varied amounts and sensitivity.

This incident has affected each institution differently. Some are less severely impacted than others. The stolen data is in many formats, some of which are easier to analyze. While the hospitals are sharing an update today, please understand that more work must be done to understand precisely which individuals and what data types were taken.

The following is an initial update on what is known to date. It is not a comprehensive report on the stolen data, as analysis remains ongoing. It is important to note this is not the official notification to individuals.

## Bluewater Health

BWH can confirm the theft of a database report. The stolen data includes information about approximately 5.6 million patient visits made by approximately 267,000 unique patients. The stolen database report did not include clinical documentation records. BWH is still in the process of determining the precise individuals included in this database report and the data that was taken and will notify those affected in accordance with the law.

While it does appear that information pertaining to employees was affected to some degree, BWH has reached the preliminary conclusion that no employee or professional staff social insurance numbers or banking information was taken. Out of an abundance of caution, since Monday October 30, BWH has been distributing two years of complimentary credit monitoring to all employees and professional staff.

## Chatham-Kent Health Alliance

CKHA's Electronic Health Record was not affected by this incident. The impacted shared drive did contain some CKHA patient information that CKHA is currently analyzing.

CKHA can confirm the theft of an employee database report containing information about 1446 individuals employed by CKHA as of February 2, 2021. If you were employed by CKHA on that date, CKHA believes that your data was taken, including name, address, social insurance number, gender, marital status, date of birth and basic pay rate. This database report does not appear to include professional staff or volunteers.

No banking information was stolen.

CKHA has been distributing two years of complimentary credit monitoring, on site, since Monday, October 30. CKHA will continue to provide this, on site, to current employees for the foreseeable future, and we encourage all employees to sign up. For those past employees included in the database report who have not signed up in person, CKHA will be mailing you a letter with your unique credit monitoring code and instructions.

## Erie Shores HealthCare

ESHC's Electronic Health Record was not affected by this incident. The impacted shared drive did contain some ESHC patient information that ESHC is currently analyzing.

ESHC has identified a limited set of stolen data that includes approximately 352 current and past employee social insurance numbers. As it does not appear that the entire workforce was affected, ESHC will be individually notifying those impacted.

No banking information was stolen.

ESHC has been distributing two years of complimentary credit monitoring, on site since Monday, October 30. ESHC will continue to provide this, on site, to current employees for the foreseeable future, and we encourage all employees to sign up. For those past employees included in the affected data who have not signed up in person, ESHC will be mailing you a letter with your unique credit monitoring code and instructions.

## Windsor Regional Hospital

A very limited portion of a shared drive used by hospital staff was accessed by the attackers. The preliminary review indicates that in the shared drive that was breached, some patients were identified by name only or some with a brief summary of their medical condition but not with any patient charts/electronic medical records.

While it does appear that information pertaining to employees was affected to some degree (i.e. staff schedules), WRH has reached the preliminary conclusion that no employee or professional staff social insurance numbers or banking information were affected. Out of an abundance of caution, since Monday October 30, Windsor Regional Hospital has been distributing two years of complimentary credit monitoring to all employees and professional staff.

## Hôtel-Dieu Grace Healthcare

HDGH's Electronic Health Record was not affected by this incident. The breached shared drive did contain some HDGH patient information that HDGH is currently analyzing.

While it does appear that some information pertaining to employees was stolen, HDGH has reached the preliminary conclusion that no employee or professional staff social insurance numbers or banking information were taken. Out of an abundance of caution, since Monday October 30, HDGH has been distributing two years of complimentary credit monitoring to all employees and professional staff.

## Next Steps

All hospitals have some degree of patient and employee information affected. All of our hospitals are diligently investigating the stolen data to determine who is impacted. This difficult process will take time. All hospitals are committed to transparency and will provide regular updates as we learn more.

The teams continue to work around the clock to restore systems. In the coming days, we anticipate providing a timeline on the restoration of operations at our facilities.

We have reported these findings to the Ontario Information and Privacy Commissioner, and we are committed to providing all those affected with notification in accordance with the law.

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 their HR teams.

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 want to thank everyone for their patience during this time.

-30-