Headwaters declares Code Grey ?All Clear? following security breach

Written By **Paula Brown**

Local Journalism Initiative Reporter

Headwaters Health Care Centre declared its Code Grey (Loss of Essential Services) ?All Clear? yesterday (Wednesday), with all of its systems now restored.

Headwaters COVID-19 Assessment Centre reopened last Wednesday (Dec. 1), after being closed due to the Code Grey being declared on Nov. 25, following unauthorized access to the hospital's systems.

As a preventative action, Headwaters shut down all of its internal systems and access to internet on Nov. 25 after the Headwaters Information Technology (IT) System and team noticed suspicious email activity.

Kim Delahunt, Headwaters President and CEO had several suspicious emails come from her account to hundreds of contacts, primarily being staff members of the hospital on Nov. 25. The email's header reads ?Welcome to Lorenz? and the email says all the files across Headwaters entire system has been encrypted, which includes private medical data.

The email continues, ?We will publish all the contents of your company on our site,? noting that this includes, ?All your confidential medical history, employers information, documentation, catalogs, reports, configs, mail, database's, invoice's, signature's etc.?

The email says to prevent the publishing of this data, visit its website and follow its instructions which entails downloading a TOR browser and paying money to recover the files.

Lorenz is a new variant of Sz40 ransomware, which is designed to encrypt data and demand ransom for decryption. This means Lorenz renders affected files inaccessible and then asks for payment to regain access.

In a press release from Dec. 8, Headwaters said cybersecurity experts continue to support the investigation into what happened and whether any sensitive data was exposed.

?This process is complex and will take some time. We are committed to being transparent and will notify individuals if we learn that any personal information has been exposed,? said the press release.

Access to Headwaters' health information system and reports have been delayed to community partners and primary care physicians as a result of the security breach.

The hospital continues to provide excellent patient care despite the recent challenges, said Delahunt in a press release from Headwaters on Dec. 3.

Surgeries and outpatient clinics have continued as scheduled at Headwaters and Emergency Department remains open 24 hours a day, seven days a week for urgent care.

Now that the Code Grey is declared over, the hospital will not be providing any further updates on the matter.