CarePartners' response:

In June, CarePartners, a home care service provider to Ontario's Local Health Integration Networks (LHINs) and an Ontario-based community health care agency, publicly reported that it was the victim of a cyber-attack by criminal actors. As a result of this attack, patient and employee information held in the CarePartners system, including personal health and financial information, was inappropriately accessed.

Acting immediately in partnership with Ontario's LHINs, CarePartners took direct steps to prevent additional exposure and close vulnerabilities. CarePartners retained a leading cyber security firm and reported to the Ontario Information and Privacy Commissioner and law enforcement officials. The investigations remain ongoing.

We are concerned that the cyber-attackers may be using the CBC to further their own extortion agenda. It is a common strategy of cyber-attackers to contact media in an effort to embarrass and shame their victims.

CarePartners takes the safeguarding of personal health and financial information seriously. At the time of the cyber-attack, CarePartners had a number of measures in place to protect the security of patient information, including:

• Its servers are managed, protected and updated by an industry leading third party;
• Its internet and firewall services were also protected by an industry leading third party;
• It had deployed ransomware protective solutions within its systems along with other anti-virus software;
• Providing employees with in depth privacy training and regular reminders about phishing emails, including how to recognize them and what to do if they believe they have received such an email;
• Utilizing a spam filter to quarantine suspicious emails received from email addresses outside CarePartners;
• Assigning system access to employees only as necessary to fulfill their role; and
• Regularly updating its systems.

Because there is an ongoing criminal investigation, CarePartners cannot provide detailed information about the nature of the attack. CarePartners can confirm that it received an email on June 11, 2018 from the cyber-attackers, and immediately took steps to validate that the information attached to the email was data that resided within CarePartners' systems.

Once verified, CarePartners (working closely with the LHINs) immediately implemented a three-stage response focused on containing the breach, notifying relevant parties and investigating and remediating the breach.

Patient and employee information held in CarePartners' computer system, including personal

health and financial information, was inappropriately accessed. Although CarePartners, in consultation with its cyber security experts, believes that the cyber-attackers do not continue to have access to its systems, there remains concern that the impacted data may be inappropriately exploited. To date, CarePartners has confirmed that 627 patient files and 886 employee records were affected. Forensics investigations are ongoing. The maximum extent of any breach with respect to patient information is the approximately 237,000 patients for which CarePartners has provided care and collected information.

In order to notify affected parties, CarePartners, in conjunction with Ontario's LHINs, issued a joint statement regarding the data breach on June 18, 2018. Additionally, CarePartners has proactively notified those patients whose records were inappropriately accessed. Affected employees were notified directly.

Throughout, CarePartners has demonstrated its commitment to patient care, and to supporting and protecting impacted employees and patients. CarePartners established a Call Centre where patients and employees can obtain further information about the breach. CarePartners is also providing credit monitoring to employees and patients for a period of one year. Information regarding credit monitoring can be obtained through the Call Centre #: 1-844-337-7300. CarePartners continues to work with law enforcement to mitigate risks to patients and employees.