M3: The Rise of E-Health Signals an Urgent Need for Cyber Coverage

December 29, 2020

- With the rise in reliance on virtual care comes the inevitable increase of data breaches. Stories of breaches abound, with the Canadian diagnostic and specialty testing company, LifeLabs, being just one example from last year.
- CBC news called the incident, which may have affected the sensitive information of millions of patients in Ontario and British Columbia, as one of “several wake-up calls” for security and privacy challenges affecting eHealth. (1) It highlights the discrepancy between the medical sector’s push for virtual care and the unpreparedness of many of these health organizations to withstand cyberattacks.
- In fact, the medical field is a prime target of hackers. According to David Masson, Director of Enterprise Security for Darktrace, hackers like to target medical facilities because these organizations are often on very tight IT budgets. "[Hackers] know they'll be struggling to actually secure their IT networks,” says Masson. “So they will see them as easy targets.” (1)

What Happens When Data Is Breached

- Electronic health records allow the sharing of necessary information between care providers across medical disciplines and institutions. But clients should know about the risks and potentially significant losses should a data break occur.
- Ransomware attacks effectively involve stealing a company’s sensitive customer data and forcing them to pay a ransom to retrieve it.
- When an organization’s computer systems are hit with an attack, it can be difficult to determine the exact extent of the damage - the exact patient files that were compromised, how many were affected, etc. This is because attackers can protect and encrypt the files they compromise. Unfortunately, this can mean a sever loss of public trust for the affected healthcare institution.
- Once a data breach has occurred, healthcare companies must pay for third-party assistance, which could compile significant costs, and might not all be covered by insurance. These costs include contracting out the help of specialized security firms to do investigative work on behalf of the company.

Measures to Protect Patients And Manage Liability Risk

- A healthcare organization should have coverage from an insurer specializing in healthcare. With so much at stake and so much to keep track of, these organizations can’t afford to overlook anything.
- As a good risk management practice, healthcare organizations should undertake a review of their available coverages and limits to ensure they are appropriate and adequate. Part of this review should include discussions with their insurance broker.

- Engaging the insurance broker as early as possible helps ensure the healthcare organization secures the right cyber coverage, resources, and expertise before an incident.
- It's also important that the insured understands not all financial losses associated with a cyber incident are covered under their general liability or property policies. Certain situations would require a separate cyber risk policy to provide adequate coverage.
- Healthcare organizations are advised to have early notification and claims reporting procedures in place to inform their insurance broker of any cyber incidents or losses. Early notification can go a long way to resolving the incident in a cost-effective manner.
- Finally, healthcare organizations should check with their insurer to confirm coverage for external legal counsel, should an incident occur.

- Visit our website for more information.
- Content is current as of the date of broadcast and is subject to change without notice.

Sources:

1. https://www.cbc.ca/news/technology/lifelabs-data-breech-security-ehealth-1.5400817