Cyber Insurance for Medical Professionals

Protecting patient data in the digital age

Why medical centres in New Zealand need Cyber Insurance

In today's digital era, cybersecurity is a significant concern, particularly for the healthcare sector. Medical centres in New Zealand rely heavily on digital systems, exposing them to cybersecurity risks. They are also custodians of sensitive patient information, making them prime targets for cybercriminals wanting to exploit patient data for identity theft and fraud.

The consequences of a cyber incident in a medical setting can be severe, disrupting operations impacting patient safety, trust and the centre's financial stability. As medical centres in New Zealand continue to embrace digital technologies, the importance of robust cybersecurity measures cannot be overstated.

What is Cyber Insurance?

Cyber Insurance, also known as Cybersecurity or Cyber Liability Insurance, is a component of a comprehensive cybersecurity strategy. It is a specialised insurance product designed to protect businesses against the financial consequences of cyber incidents. This includes coverage for data breaches, ransomware attacks and other digital threats, helping to manage financial fallout and access incident response services for quick recovery.

While IT providers work to implement robust cybersecurity measures, Cyber Insurance provides a financial safety net when breaches occur. One usually complements the other, as Cyber Insurance can often cover the costs of services provided by IT experts to address and mitigate incidents.

How Cyber Insurance can offer protection for medical centres

1. Data breach cost recovery

Medical records contain personal and medical information that can be exploited for identity theft, fraud and other malicious activities. Cyber Insurance helps medical centres manage the costs associated with data breaches. This includes notifying affected individuals, claims made by patients whose data has been compromised, providing credit monitoring services, and addressing legal liabilities.

2. Financial safeguard

The financial impact of a cyber incident can be devastating. In addition to immediate costs like cyber extortion, system restoration and legal fees, medical centres may face long-term financial consequences such as regulatory fines and reputational damage. Cyber Insurance provides a financial safeguard, helping centres recover and continue their operations.

3. Access to expertise

Managing a cyber incident requires specialised knowledge and skills. Cyber Insurance policies often include access to cybersecurity experts who can assist with incident response, forensic investigations, Privacy Act and reporting obligations, and public relations. This expertise is invaluable in mitigating the impact of a cyber incident and preventing future breaches.

Cybersecurity incident example

There have been several high-profile cyber incidents in New Zealand, that have highlighted the vulnerabilities of the healthcare sector. The following example shows how a medical practice email can be compromised and used for phishing scams.

Medical practice (unnamed for privacy reasons): Email compromise

A medical practice discovered their email had been compromised and used for phishing. They changed the password immediately but were unsure how long the intruder had access.

The compromised email was used for sharing patient information, reports, referrals, payment details and medical histories. Forensics found a third-party application that could copy the entire mailbox to the intruder's device.

Forensic costs of $10k were covered by Cyber Insurance. Public relations support was needed to manage media and stakeholder communications, with $2k in costs covered. Legal counsel provided privacy advice, drafted notifications for government bodies and individuals, and conducted electronic discovery (eDiscovery) on the compromised mailbox. Total legal, eDiscovery and notification costs of $153k were covered by the medical practice's Cyber Insurance and IDCARE was engaged to support affected individuals.

Reference: Emergence Insurance

How MAS can help

MAS has a team of business risk specialists and a Cyber Insurance specialist, to help place Cyber Insurance for our Members. We assess your business risks, find suitable providers, recommend necessary covers and manage these covers for you.

To learn more or to speak with our Cyber Insurance specialist, ask your MAS Adviser or email businessinsurance@mas.co.nz.