+BUSINESS | In print

Protect your healthcare practice: How to take vital steps against growing cyber threats

Craig Simpson

Monday 27 November 2023, 03:58 PM

2 minutes to Read

Cybercrime is on the increase, and healthcare practices are particularly vulnerable [Image: FLY.D on Unsplash]

I've heard that practices like ours could be given hefty fines and be liable for costs if we don't adequately protect our patients' personal information. What should we do?

– Responsible, Wellington

Cybercrime, one of the fastest-growing criminal activities worldwide, poses a significant threat to the healthcare industry. New Zealand businesses are not exempt, making robust protection imperative in the face of constantly evolving cyber threats.

Data breaches can result in a significant disruption to your business, negatively impacting you, your colleagues and your patients or clients. There are several things you can do to keep yourself and your patients' information safe from cybercrime. These include choosing unique passwords, checking privacy settings, staying on top of all software updates, and using two-factor authentication (2FA).

Deputy privacy commissioner Liz MacPherson recently made it clear that if you hold personal information under the Privacy Act 2020, you are responsible for taking all reasonable measures to protect this information from cybercriminals. Ms MacPherson has indicated that the minimum reasonable requirement for all small businesses or organisations that hold or share personal data digitally would be 2FA.

You may be found in breach of the act if you are a small business that has a cyber-related privacy breach, and you don't have 2FA at least in place.

What is reasonable depends on the size of the organisation, the amount of personal information held and the sensitivity of the data. Any scale of information or sensitivity will require protection over and above the minimum standard 2FA.

2FA is another layer of security between the information you hold in digital format and the people who want to steal or use this information unlawfully. The 2FA can be an additional password received by text to the user's mobile phone or email address.

A privacy breach is when someone's personal information is accessed, altered, disclosed, destroyed or lost without permission or by accident. It is a serious matter that can have legal consequences for the organisation or individual responsible.

There may be different remedies available for the affected parties depending on the nature and severity of the breach.

However, by not having 2FA in place, you may violate the act and be liable for a fine of up to $10,000.

The privacy commissioner may issue a compliance notice to organisations or businesses that must meet their obligations under the act. There is also an option for the commissioner to “name and shame” should they feel it is in the public’s best interest.

Most cyber insurance policies require the policyholder to comply with legislation or any public authority acts and regulations. This means the policy will not respond if you are seen to be in breach of the act.

It is important to make sure you review your cyber insurance coverage to ensure you have appropriate protection for cyber losses, including business interruption cover, the cost of restoring data, forensic data examination, network extortion cover, hacker theft cover, legal defence costs, third-party liability and privacy-breach cover.

Craig Simpson is head of business risk and advisory services, MAS

Michelle, capture your time to Read, Watch, Listen or Delve by clicking CAPTURE.

CAPTURE

You can view your CAPTURE RECORD here.