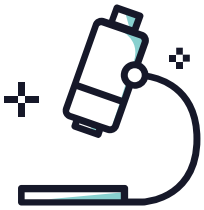
Cyber checklists

INDUSTRIES

wotton kearney

A founding member of LEGALIGN GLOBAL



Health

As a healthcare provider you hold highly sensitive private information that may be the target of cyber-attacks. Making sure your organisation is cyber ready is imperative to reducing your risk as a business. It is important that you:

1. understand what data you hold;
2. understand general cyber risks and those specifically relevant to your industry;
3. take steps to reduce your cyber risk; and
4. be prepared to respond to cyber-attacks if that occur.

Understand your data

Understanding the data you hold is an important part of effectively assessing and reducing your cyber risk. As a healthcare provider you are likely to not only hold financial information for your clients, but also medical records, which are of an extremely personal and sensitive nature. You should aim to be aware of the volume and type of information you hold for each client and whether that is their complete medical file or only isolated records, in order to effectively assess breaches and whether you need to notify clients, and what you need to notify them about. You should also have a policy about how long you retain your clients' information and where that information is stored.

In the event that sensitive data is compromised in a data breach, a number of risks can potentially arise for your organisation and your clients, including financial, physical, psychological and reputational harm. Depending upon the depth of information you hold about your clients, they may also be exposed to financial harm arising from identity theft. You will need to consider whether this amounts to a risk of "serious harm" and whether the incident is notifiable under the Notifiable Data Breach Scheme set out in the Privacy Act (click **here** for more information).

Understand your risks

You should be particularly wary of cyber-attacks in the form of ransomware and data scraping. Ransomware is malware which encrypts the data on your systems and then demands money in exchange for being decrypted or unlocked, whereas data scraping is where an attacker enters your network to access and export your data. Sometimes, these attacks can occur at the same time, meaning the hacker is able to exfiltrate your data while before your data is encrypted and you are unable to access your systems.

These attacks usually start through phishing attacks, where fraudulent emails are used to trick users into revealing their login information or giving access to their network account or getting them to download malware through a document attachment or link.

Reduce your risk

There are two major areas to focus on to reduce your cyber risk: security systems and employee training.

Security systems

Accepting that not all cyber risks can be eliminated, there are steps you can take to reduce your risk. You should consider seeking the assistance of your IT provider about:

+ Setting up alert systems for suspicious or abnormal email activity.
+ Turning on comprehensive audit logging in your email systems.
+ Requiring employees to update their passwords regularly.
+ Locking user accounts after 3 failed password attempts.
+ Enabling multi-factor authentication.
+ Configuring regular back-ups of your data and regularly testing those back-ups. Ideally, these back-ups will be disconnected from your main server in case your main server is attacked.
+ Regularly updating firewall and anti-virus software.
+ Application whitelisting.
+ Patching applications immediately when a patch is available.
+ Configuring macro settings.
+ Restricting administrative privileges.

Employee training

The single biggest cause of cyber breaches is human error – be it inadvertently downloading malware from email attachments or handing over credentials via genuine looking websites. Therefore, a critical element in safeguarding your systems is employee training.

Training should be organised through your IT provider and be regular and customised according to your systems and internal structures. Training ensures that every employee understands that cyber safety is part of their responsibility and that individuals are on the alert for external threats. Have specific cyber training for employees identified as incident responders in your incident response plan.

See our comprehensive guide on cyber readiness **here**.

Respond to attacks

Responding to cyber-attacks is a three-stage process, outlined in our **Guide to Cyber Breaches**.

As a healthcare provider you will be required to notify the OAIC and affected clients of eligible data breaches under the NDB Scheme, which supplements the mandatory data breach reporting requirements of the My Health Record system for branches that occur outside of the My Health Record system.

Breaches that occur within the My Health Record system should be notified and dealt with through the Australian Digital Health Agency. You may also have additional obligations to report to the Commissioner under the National Cancer Screening Register Act.