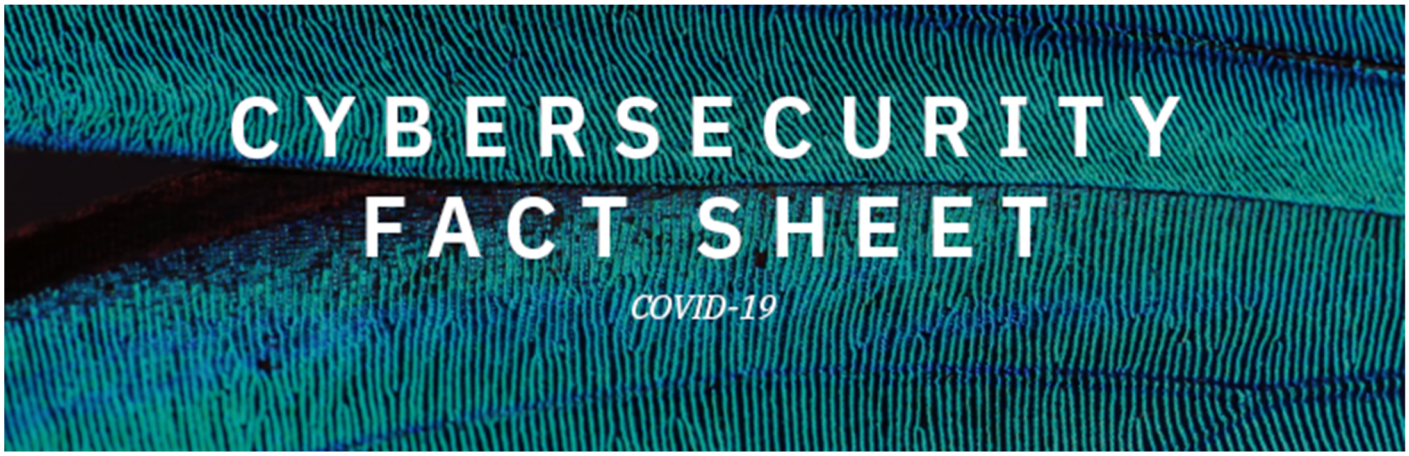

Moving from in-person consultations to telehealth can create security risks, especially when using personal devices. Opportunists are already using COVID-19 as a subject matter for phishing scams, hoping the unsuspecting will disclose personal information.

The Office of the Australian Information Commissioner's (OAIC) latest report of notifiable data breaches (July - December 2019) demonstrated that health service providers accounted for 21% of reported data breaches. This was higher than any other industry. Therefore, it is important for health practitioners to familiarise themselves with cyber security risks, to ensure that patients' privacy, confidentiality and trust is maintained.

Legal considerations

Health practitioners need to be aware of their obligations under the Privacy Act.

These include:

- Health service providers must notify affected individuals and the OAIC about any data breaches that are likely to cause serious harm
- Practitioners must take reasonable and active steps to ensure that personal information is collected, stored, used and disposed of in a manner that protects privacy
- Practitioners must ensure that the platforms used for communicating with patients are safe and secure

How can health practitioners protect themselves against data breaches?

Practitioners can take a number of steps to guard against a potentially costly data breach:

- Be cautious of any COVID-19 themed email seeking personal information. Look for the tell-tale signs of a phishing email, namely spelling or grammatical mistakes in the text and generic greetings. Always verify an email address before downloading or clicking on an email link. If you are unsure, don't open and call a colleague!

- Ensure you have strong password protection on both your devices and platforms, such as two-factor authentication. Platforms used should use end-to-end encryption. Log out and lock your screen when not in use and don't leave your device unattended. Ensure your device has anti-virus software in place and keep it fully updated.
- Clinics can create policies prohibiting work on public networks or restricting public access through VPN connections only. Further, clinics should communicate cyber security policies to employees clearly and frequently and conduct remote training as necessary.
- Define and communicate a clear procedure to follow in case of a security incident and provide adequate support.

Further, health practitioners should continue to maintain appropriate record keeping by ensuring that all emails and other digital information are saved to patients' clinical records.

Good cyber security will guard against data breaches, like good hygiene will curb the spread of COVID-19.

Colleen Palmkvist
Partner

Jane Fiske
Partner

Anna Murray
Lawyer