COVID-19, REMOTE WORKING AND THE HEALTHCARE SECTOR

Written by Jehan Mata, Special Counsel, located in Melbourne, and Edward Osborne, Special Counsel, located in Sydney

Coronavirus (**COVID-19**) has resulted in rapid changes to the way workplaces operate, and our healthcare providers are no exception to this. As the use of remote-access technology becomes more widespread, healthcare providers may become more vulnerable to cyber-attacks, which may in turn lead to privacy-compliance issues and service interruptions. It also presents other risks for providers, including the potential for litigation due to misdiagnosis or changes to communication methods.

Virtual-care limitations and risks

In response to COVID-19 and limitations around in-person consultations, the Medicare Benefits Scheme (**MBS**) was recently expanded to allow for an increase in telehealth consultations, meaning that virtual care will no longer be limited to patients in rural settings.

One of the key limitations in conducting virtual examinations is the ability of the patient to access the appropriate technology. Many patients now required to use telehealth facilities are elderly and immuno-compromised. Unfortunately, older patients often do not have smartphones, adequate internet connections, or the ability to navigate the technology. This may discourage practitioners or patients from engaging in telehealth appointments.

The inability to perform a physical examination also provides a major challenge for practitioners. Virtual assessments likely increase the chance of misdiagnosis, which is arguably the greatest liability risk telehealth presents. To ensure practitioners adequately discharge their duty of care, it is imperative that they inform patients of the limitations in making diagnoses and recommending treatment if the patient is seen remotely.

The difficulties performing remote assessments may prompt health practitioners to make alternative and provisional diagnoses, with follow-up advice to patients to arrange an in-person visit to an office for lab tests and a physical examination.

The widespread use of telehealth may also lead to performance or conduct-related complaints to the Australian Health Practitioner Regulation Agency (**AHPRA**). As noted earlier, there is an increased risk of misdiagnosis associated with virtual examinations, and such issues are often referred to the regulator for investigation. Communicating and building rapport with patients can be particularly challenging at times, which could increase complaints made to AHPRA. Accordingly, practitioners should take care to maintain accurate and up-to-date records and consultation notes, as this may assist in protecting practitioners from exposure or from disciplinary action should future claims arise.

Privacy and cybersecurity considerations

On 31 July 2020 the Office of the Australian Information Commissioner (**OAIC**) released its half-yearly notifiable data-breach report, revealing 518 data breaches were notified to it in the six-month period to 30 June 2020. The healthcare sector featured heavily, making up 22% of all such notifications. In fact, since OAIC reporting started in 2018, the healthcare sector has

consistently notified more data breaches than any other sector.

Two days after the release of the notifiable data-breach report, the Australian Cyber Security Centre (**ACSC**) advised of a significant increase in targeted ransomware campaigns against healthcare providers, which include a data-stealing component.

Then, on 6 August 2020 the Commonwealth Government released its 2020 Cybersecurity Strategy (**Cybersecurity Strategy**), which, among other things, recognised the criticality of the healthcare sector, and the importance of mitigating cyber risk and maintaining strong privacy safeguards in it.

Privacy and cybersecurity in the healthcare sector are nothing new; healthcare records often contain highly sensitive information, so are attractive to cyber criminals and insider misuse, and otherwise subject to elevated privacy-protection obligations.

So, what can healthcare providers do to improve their privacy and cybersecurity posture?

On the governance front, our proactive clients will have established or be working on establishing:

- an appreciation of the intersection between cybersecurity and privacy and, in relation to the latter, a plan to comply with the Australian Privacy Principles or other relevant statutory privacy frameworks
- an understanding about how data is processed, and the privacy and confidentiality interests of stakeholders served or affected by them
- privacy and cybersecurity risk assessments, allowing them to prioritise and act on identified risks
- a privacy and cybersecurity governance framework, and granular controls for understanding and managing their risk-management priorities
- a plan to communicate the importance of privacy and cybersecurity to stakeholders, and how they deal with each, and
- appropriate data safeguards.

While we generally do not provide technology-focused cybersecurity advice, there are several freely-available resources that can serve as a good starting point. One such resource is the ACSC's website where you can find details about the "Essential Eight"—a series of baseline cybersecurity mitigation strategies to fend off such attacks in the future.

Embracing technology increases availability of medical services

Despite the ongoing challenges of COVID-19 and remote working practices within the healthcare sector, the increased use of technology to connect with patients and otherwise streamline their care helps the availability of medical services to, for example, people in remote and rural areas.

Understanding the risks associated with more reliance on technology and mitigating against them can seem daunting. However, ensuring business continuity—and limiting the likelihood of data loss, liability or regulator intervention—are strong motivators for a proactive compliance approach.

Acknowledgement: Brydee Hodgson, Lawyer, Paul Scopacasa, Lawyer and Deborah Placidi, Paralegal