THE CYBER SUPERSPREADER - MOVE OVER COVID, THERE IS A NEW VIRUS IN TOWN AND IT'S HERE TO STAY

Authors: Partner Mark Doepel and Special Counsel Jehan Mata

In March 2020, there was a tremendous shift as consumers and providers looked for ways to safely deliver healthcare electronically during the pandemic. In May 2021, 17% of services were delivered virtually and it is expected that digital health will continue to be used to deliver care. That said, the virtual platform is not novel and the shift to digital health was underway prior to the pandemic. Unfortunately, the transformation in the health industry is not the only change we have seen during the pandemic. There's also been a surge in cyber-attacks on the health sector as cyber-criminals take advantage of the pandemic.

The Australian Cyber Security Centre (ACSC) has reported an

increase of about 85% of cyber security incident reports

in 2020 as compared to 2019.

Reports of these attacks came from both health care professionals and customers who fell victim to data breaches and health related scams. This article discusses the current trends, the threats that the medical industry is facing, and the steps required to remain vigilant and safe.

Digitalisation and pre-pandemic changes to health sector

Many industries, including the health sector, have made a significant move to digitalisation in the last two years. Australia has adopted advanced technology during the pandemic, allowing practitioners to deliver healthcare—in the large part—safely to Australians.

My Health Record was introduced in 2012 to provide a platform to store a digital copy of personal medical information within an online national database. It allows consumers to manage their medical record, add additional information and share their record with multiple practitioners with the aim of providing seamless, safe and efficient care.

By 2016, the My Health Record service had

2.6 million users

which is nearly 10% of Australia's current population.

Another service introduced in May 2013 was myGov, which provide Australians with one secure platform to access a range of services. This integrated Federal Government database saves time, paper, personnel and has a long-term lower expenditure. These are just a couple of examples of moves within Australia to a more digitalised healthcare system prior to COVID-19.

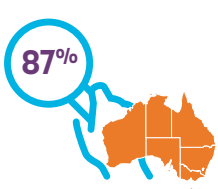
Health sector since the pandemic

When the virus hit, the healthcare system was placed under immense pressure to deal with this unprecedented and evolving landscape. As a result, the government fast-tracked its plans to provide secure platforms, such as telemedicine for medical professionals. To augment these changes, Medicare also made additions to its list of reimbursable covered services, so as to allow practitioners to be remunerated for providing care virtually until 31 December 2021.

These changes to the Medicare Benefits Schedule (MBS) have assisted in the provision of continuous and coordinated healthcare and high-quality practices. More than four million health and medical services have now been delivered to more than three million patients through MBS telehealth items.

In the United States, telehealth usage has increased 38 times from the pre COVID-19 baseline.

In just April 2020, the **application of telehealth was 78 times higher** than in February 2020.



Similarly, Australians have been responsive to telehealth, with **87%** of consumers reporting an interest in continuing to use telehealth if Medicare funds it.

Medical practitioners also hope that the current funding arrangements will remain. At the time of publication, the government has yet to comment on whether MBS telehealth items will become a permanent feature.

Cyber-attacks and ransomware

As telehealth becomes an increasingly important element in the provision of health services, so too does the increased risk of cyber-attacks and ransomware. Consequently, cyber-attacks and security breaches have become an extreme concern as cybercriminals take advantage of the pandemic environment. The health industry has been a lucrative target for cybercriminals, as personal information is in high demand on the dark web. These cyber-attacks can result in patient information being accessed, leading to possible identity theft, data extortion, reputational harm and other damage. Security breaches can cause significant financial loss and possible legal liability.

Therefore, it is vital for businesses and individuals to be alert as cybercriminals continue to evolve their craft.

An increase in phishing attacks are occurring, noting that **91% of cyber-attacks** begin with a phishing email.

The increase of email related breaches in the health sector has been overwhelming, especially in smaller businesses, with 59% reporting phishing attacks. Cybercriminals target small businesses because they don't always have the financial ability to invest in advanced technology or provide cyber training to their staff. Sixty per cent of people also report working in distracting environments, with 73% of employees making more mistakes due to general fatigue experienced during the pandemic.

Against this backdrop, businesses and individuals need to be hyper-vigilant to reduce the risk and impact of a cyber-attack. In a recent case, a pharmacy staff member clicked on an email thinking it was from a supplier and within minutes all PCs were locked with an accompanying ransomware demand. The pharmacy could not dispense or trade. Fortunately, the business IT provider already had precautions in place and had backed up the pharmacy's data. These precautions allowed the pharmacy to continue trading within 24 hours of the cyber-attack. However, this did not stop the business from incurring financial loss and reputational damage. This case highlights the importance of creating a culture of cyber-awareness and adopting good security practices as part of day to day activities.

At their worst, these attacks can be a threat to patients' wellbeing and lives. The United Kingdom's National Health System hospitals suffered a ransomware attack in 2017, forcing them to delay treatment plans and reroute incoming ambulances as they lost access to the hospitals' information systems. These attacks impede hospital operations and put the health and welfare of patients at risk, making clear that a new level of caution is essential to reduce the risk of attack. Refer to our recent article Ransomware - Show me the money: should we or shouldn't we that explores legalities of Ransomeware.

Practitioners' duty

All healthcare providers have a professional and legal obligation to protect their patients' health information. Creating and maintaining information security practices is a critical professional and legal obligation when using digital health systems. The *Healthcare Identifiers Act 2010* requires reasonable steps to be taken to protect healthcare identifiers from misuse, loss, modification, disclosure and unauthorised access. The *Privacy Act 1988* (Cth) outlines the privacy responsibilities with which healthcare providers must comply in managing health and personal information. Noncompliance with healthcare provider requirements can result in civil penalties and/or imprisonment. The Department of Health published a checklist for telehealth services to help healthcare providers maintain privacy and confidentiality whilst using technology-based consultations. The list below sets out some ways practitioners can provide safe and effective health services via telehealth whilst maintaining confidentiality:

- Assess whether telehealth is safe and clinically appropriate for the patient and whether a physical examination is required to provide better care.
- Configure and establish web conferences and phone calls securely.
- Identify yourself and confirm the identity of the patient. Be aware of unidentified participants and surroundings.
- Ensure protection of patient's privacy and their rights to confidentiality, particularly if working from home.
- Maintain clear and accurate health records of consultations.

Benefits of digital health

Digital health in combination with good practice and safety measures provides significant benefits to the Australian economy. The digitalisation of medical data enables high quality healthcare, which include:

- responsive and sustainable healthcare
- prevention before treatment, as digital health aid patients to self-manage their conditions through regular monitoring and tracking of symptoms
- avoiding hospital admissions
- reducing time spent in waiting rooms
- fewer adverse drug events
- less duplication of tests
- fewer medical errors
- improved coordination of care for people with chronic and complex conditions
- better-informed treatment decisions, and
- expanding the reach of healthcare professionals.

Healthcare also contributes 5% to global greenhouse gas emissions. The use of digital health reduces the dependence on paper-based communication, which lowers healthcare's carbon footprint.

Studies show that an increase in **digital health over the past six years has resulted in a decrease in greenhouse gas emissions**. So not only does digital health provide efficiencies and enhance healthcare, it is also good for the planet.

Necessary precaution and safety measures

With every benefit comes a risk. The surge in cyber-attacks and ransomware means that a new level of vigilance is required, and appropriate measures are necessary. It is highly recommended that businesses obtain cyber insurance, as part of a suite of policies. Ultimately, it is important to understand that cyber-attacks cannot be prevented; nevertheless, we can reduce the impact they have on us. This is achieved by backing up data, updating systems regularly, staff training and creating a self-awareness culture.

Takeaway

Change is and was inevitable, and the digitalisation of healthcare was already on its way. The pandemic has certainly accelerated the process and has seen the government introduce technology almost a decade earlier than planned. However, the health industry's exposure to attack is still high and it is everyone's responsibility to be proactive and remain vigilant to ensure a sustainable and safe transition to digital health. Ultimately, prevention is better than cure and ongoing vigilance and resilience will assist the industry moving into a more digitised world.