beazley

Article

Digital health: the unstoppable revolution that brings new emerging risks

Pilar Gonzalez • October 24, 2023

The COVID-19 pandemic sparked a shift where traditional healthcare's physical environment was adapted to a digital environment in order to maintain healthcare activity during lockdowns and other disruptions to everyday life. Subsequently, the pandemic has proved to be the accelerator for the technological revolution that the Healthcare and Life Sciences sectors are undergoing.

According to Global Market Insights, the digital health market was valued at US$210 billion in 2022, and is forecast to continue growing over the coming years, exceeding US$800 billion by 2030.[1]

In an era of constant and rapid change, new terms are being coined in which technology, AI and virtual reality are intermingled: i-health, m-health, telemedicine, video consultations, home-spitals, chronic disease monitoring apps, care and health apps, even medical records with digital signatures.

What until now was simple to categorise has become substantially more complicated. Where can we classify these types of company? Are they health or technology companies? And what regulations apply? For example in Europe - Article 46 of Spanish Law 44/2003, of 21 November, on the Regulation of Health Professions[2] - states that "health professionals practising in the field of private healthcare, as well as legal persons or privately owned entities that provide any kind of healthcare services, are obliged to take out the appropriate liability insurance, a guarantee or other financial guarantee to cover any compensation that may arise from any possible damage to people caused by the provision of such care or services."

Digital health services and products create a specific set of risks that traditionally have not always been linked together – cyber, tech and reputation, data breach and product liability, and medical malpractice

(med mal) and media liability, as well as professional indemnity.

This combination of risks reflects the reality of the digital health sector today.

For example, tech businesses typically understand cyber and data breach liabilities and product liability, but they are perhaps less aware of the med mal, professional indemnity and bodily injury risks they may face. Whereas healthcare providers understand their professional med mal liabilities but have never had to consider cyber and product liability risks previously.

Cybersecurity in Healthcare: still in the ICU?

As a sector that is rich with personal individual data, but without the cash to widely invest in modernised security infrastructure, the Healthcare sector is uniquely exposed to cyber-attacks. This risk was evidenced in Check Point Software's Cyber Security Report 2022,[3] which identified that the global Healthcare sector suffered a 74% increase in cyber-attacks last year.

Beazley's own Risk & Resilience research also revealed that of the Healthcare and Life Sciences businesses we surveyed, 32% did not feel prepared to manage and respond to cyber risk. In addition, 74% of Healthcare and Life Science sector business leaders think cyber will be one of their top three concerns in 12 months' time, which provides further insight into the low levels confidence that businesses in this sector have in their ability to combat cyber risk.[4]

In addition, Healthcare is a sector that cybercriminals focus on as they seek to steal valuable Intellectual Property (IP). Our research also found that 70% of Healthcare and Life Sciences executives ranked IP risks within the top three most significant technology risks affecting their business, demonstrating the importance of IP in this industry.

These statistics underline the need for Healthcare and Life Science companies that are operating in or seeking to expand into the digital health space, to ensure that their insurance coverage is designed to suit all the risks their business will face from med mal liability risks through to product errors & omissions to cyber risks. Beazley's Virtual Care cover has been designed with this in mind, and it offers three pillars of coverage – Medical Liability, Technological Liability and Cyber Protection, and includes coverage for personal damages that occur as a result of a cyber-attack.

Here are some examples of what can go wrong and the risks that digital health companies face.

mhealth (mobile Health)

An app designed to check and detect signs of cancer on patients' skin through photographs and AI-based technology, failed to detect cancerous lesions leading to a patient Medical Liability claim.

Technology risk

A software company specialising in medical data conversion from an updated electronic medical records program failed to correctly transfer the medical records of a patient who was prescribed the wrong medication, causing them physical harm.

Cyber risk

In July, a Tennessee-based Healthcare organisation fell victim to a data breach, which compromised the personal data of over 11 million patients across 20 US states.[5]

In the UK, a ransomware attack caused widespread outrages across the NHS in August 2022.[6] The attack targeted a software supplier and affected a host of core services, including ambulance dispatch, out-of-hours appointment bookings and emergency prescriptions. This incident followed a ransomware attack on Ireland's state health services provider in May 2021, which caused widespread disruption for patients as workers were forced to work with paper records as the IT systems were targeted.[7]

An unstoppable revolution

Digital healthcare is an unstoppable revolution that requires both new regulations to regulate this new and burgeoning industry, as well as insurance solutions designed to meet the emerging risks digital health organisations and technology companies creating new health solutions and services face. At Beazley we understand the challenges and recognise the risks which is why we offer tailor-made products designed to support the sector and the myriad of organisations within it.

[1] Digital Health Market Size, Share, Growth, Trends Analysis & Forecast (beyondmarketinsights.com)

[2] Law 44/2003, Of 21 November, Management Of The Health Professions.

[3] Check Point 2022 Cyber Security Report

[4] Spotlight On Cyber and Technology Risks 2023 | beazley

[5] Biggest Healthcare Industry Cyber Attacks | Arctic Wolf

[6] NHS ransomware attack: what happened and how bad is it? | Cybercrime | The Guardian

[7] Cyber-attack on Irish health service 'catastrophic' - BBC News

Pilar Gonzalez

Underwriter - Int Miscellaneous Medical & Life Sciences

beazley