Intro to digital health insurance
What is digital health?

Digital innovation is set to transform the face of healthcare across the world. Ground-breaking new ideas and tools have the potential to offer patients faster, more accessible and more efficient care, which can only improve the healthcare system as a whole. While there will undeniably be obstacles to overcome, the future of healthcare is bright.

Digital health includes subsectors such as interactive telemedicine, mHealth (healthcare related mobile apps), artificial intelligence, remote patient monitoring, genomics and many more. Businesses operating in the digital healthcare arena can range from traditional doctors’ offices and hospitals, to insurance companies, device manufacturers and myriad software companies.

Today, you can talk to an AI-powered chatbot, diagnose your illness online or even order a prescription from the comfort of your own home. With technology predicted to replace as much as 80% of a physician’s everyday routine\(^1\), the reliance on technology in healthcare has never been so great.

\(^1\) https://fortune.com/2012/12/04/technology-will-replace-80-of-what-doctors-do/
The need for bespoke insurance

As the healthcare and technology sectors continue to intertwine, practitioners and companies operating in the digital health space will start to experience a wider range of risks. From misdiagnosis of medical conditions, due to the distortion of x-ray images sent using store-and-forward technology, to incorrect readings of glucose monitors leading to patient harm.

So what does this mean for the insurability of practitioners and companies operating in digital health? Well, in short it becomes problematic. Medical malpractice insurers are rightly concerned about the potential for patient harm arising from technology-related errors, not to mention the lack of credible data to nullify their concerns for it eroding their profit margin. As a result, their policy triggers have stayed eye-wateringly static despite the global rise of technology within healthcare.

This has already, and will continue, to lead to gray areas within insurance placements. The knock-on effect of this will be finger-pointing between three or more insurers over the proximate causation of the loss: was it a healthcare incident, technology error or cyber event? Absent any case law, and despite the litany of disclaimers, companies will then subsequently be required to pay three different deductibles and may even run the risk of having no coverage whatsoever. The debate will then intensify about who makes the ultimate decision on patient care, the technology or the traditional healthcare provider?

With these sentiments in mind, the insurance industry is on the cusp of a more modernized approach for healthcare providers. It has become crucial for brokers to advise their clients of these potential pitfalls in standard insurance policies, and to source policies tailored to their clients’ unique needs.

A dearth of affirmative coverage is present in the insurance industry for traditional healthcare providers and digital health companies alike.

Technology E&O insurers will only extend to losses arising from 'technology activities' and are loathe to offer any form of bodily injury whether it’s on a primary or contingent basis, and cyber insurers typically exclude all forms of bodily injury.

Want to know more? Get in touch healthcare@cfcunderwriting.com
Key exposures for digital health

Companies operating in this space often bridge both the healthcare and technology sectors, and while the traditional exposures of medical malpractice, professional liability and general liability are still present, the integration of technology creates emerging threats and heightened privacy concerns.

Bodily injury (medical malpractice)
Healthcare providers are facing new threats to their patients as technology advancements continue to play a more crucial role in how healthcare is delivered, monitored and addressed. A modern policy should provide coverage for bodily injury arising from not just the provision of healthcare and technology services, but also cyber events and system outages.

Technology E&O
Technology is fundamentally changing healthcare. The supply, development, installation and maintenance of technology has become a pivotal component in the digital health industry and in turn could be a key exposure.

Products failing to perform
Wearable technology has a prominent role in today’s healthcare, especially delivery, which is bringing remote care to the patient. Any tangible product that has been manufactured, altered, distributed or installed by a digital health company, including wearables and self-monitoring healthcare devices, should be covered.

Cyber and privacy
Cyber and privacy coverage should be tailored to address digital healthcare companies’ specific cyber exposures. Not only should it include a separate section for extortion to address the growing threat of ransomware, but it should also extend to regulatory fines and penalties and include initial response services with a nil deductible.
Intellectual property rights infringement

Intellectual property (IP) cover is vital in protecting the value of any digital healthcare companies’ assets and brand. Infringement of IP rights, such as copyright allegations or trademark infringement, as well as damages, settlements and counterclaims can be extremely costly.

Changing nature of bodily injury

Traditional bodily injury coverage triggers have become outdated and are no longer sufficient with the global rise of technology.

Healthcare services

Failure to adequately assess a patient and their symptoms via telemedicine could lead to incorrect diagnosis and delayed treatments. Similarly, if a patient is sending a picture of a physical issue, such as a rash, a distorted image could lead to an incorrect diagnosis.

Technology activities

Artificial intelligence is now being used to more effectively triage patient conditions, most commonly diagnosing basic illnesses via a chatbot function. However, the way in which a patient describes their symptoms can leave the chatbot confused or the patient undiagnosed.

Cyber attack

A targeted ransomware attack could deny access to systems and patient data, where patients’ vitals are being monitored and medications are prescribed via telemedicine. If a cyber attack cripples the telemedicine system or electronic medical records database, patient records could be lost or patients could be prescribed the wrong medication leading to death.

System outage

A failed update or computer system outage could affect remote patient monitoring functions. This could pose a risk to patient’s safety in the event of a medical emergency.
Policies in action

AI chatbot
A patient was registered with an online health platform and regularly used it to book appointments with physicians. The platform had recently introduced an AI chatbot function which allowed patients to be quickly and efficiently treated. On one occasion the patient used the AI chatbot function and was misdiagnosed, which lead to a costly and lengthy follow up process for both the patient and the online health platform. The output of AI is only as good as its human input and often when AI programmers do not have a medical background or training, there is an increased likelihood for false positive and false negative errors to occur.

Medical imaging
A medical imaging company created a mobile application which is used by teleradiologists. In this event - which eventually led to death - a patient experienced trauma due to slow treatment caused by the delay in image availability via the app. Although both parties were sued, it was alleged by the reporting facility that the death of the patient was due to a slow transfer of images from modalities connected to the radiology picture, archiving and communications system.

Interactive telemedicine services
A physician tried to access a patient’s medical records using a third-party healthcare information exchange (HIE). The physician was unable to retrieve the patient’s medical records due to the HIE being hit with a ransomware attack and being taken offline. Instead, the physician manually completed a health questionnaire via telemedicine, and then prescribed antibiotics to the patient. It transpired that the patient had misinformed the physician that they were allergic to penicillin, resulting in their death.
All information in this booklet is correct as of 01 September 2019. We take great pride in our professional expertise on digital health insurance and as such would like to state that certain content within this document is liable to become outdated due to the fast-paced nature of the insurance market.

CFC is a specialist insurance provider and a pioneer in emerging risk. With a track record of disrupting inefficient insurance markets, CFC uses proprietary technology to deliver high-quality products to market faster than the competition while making it easier for brokers to do business. Our broad range of commercial insurance products are purpose-built for today’s risks, and we aim to give our customers everything they need in one, easy-to-understand policy.

Headquartered in London, CFC serves more than 70,000 businesses in over 80 countries. Learn more at cfcunderwriting.com and LinkedIn.

To contact us, please email inbox@cfcunderwriting.com or dial +44 (0) 207 220 8500. Our healthcare team can be reached via email on healthcare@cfcunderwriting.com.