beazley

Telehealth: a growing field and an evolving risk landscape

Jennifer Schoenthal and Dakai Pouncey

25 January 2022

Few industries have seen more dramatic growth in recent years than that of virtual care. Telehealth's benefits – including improved access and affordability – have been hard to deny, ensuring that the virtual care industry is here to stay. With this new host of services, however, comes an evolving risk landscape that includes a wide range of cyber and technology-related exposures.

Understanding the full range of telehealth risk exposures can be challenging for newcomers to the space. Just as telehealth technology companies may be less familiar with bodily injury and medical malpractice exposure, medical companies may need help navigating technology errors and omissions and cyber risk.

First party cyber and tech risk exposures and claims

When it comes to telehealth-related vulnerabilities, cyber and related data security and privacy exposures are key concerns – and can be extremely varied in both cause and severity.

Devices can be hacked, as can record storage, but while people generally envision only this kind of high-profile incident, the source of a breach can often be far more innocuous. Data breaches can stem from circumstances as simple as a doctor leaving a laptop on a train or a family member overhearing confidential patient information when a practitioner is working at home. And don't forget the trickle-down factor; if a platform provider goes down, no one on the platform will be able to do business.

Ransomware, one of many cyber exposures a telehealth company may face, can prevent healthcare providers from accessing the patient information that they need to provide continuity of care. But victims don't necessarily need to be major health systems; if the developer of a health-related app has their code locked up by a hacker, they are unable to conduct business as

well. When a ransom attack occurs, incident response (i.e. privacy, forensic, crisis management) is needed to understand the extent of the compromise and assess if the sensitive information involved trigger any breach notice laws. Claims support should always include assistance with finding negotiators, facilitating data restoration, or initiating hardware replacement as needed - essentially doing whatever is necessary to bring the insured back to a pre-breach state.

When building an integrated product with multiple coverages, a strong underwriter must focus on all towers of coverage equally, which means wearing many different hats while underwriting telemedicine: medical malpractice, technology, media, general liability and cyber. But because of the interconnected nature of tech-related exposures, many virtual care claims do tend to have a cyber component to them. Brokers and their clients are well advised to work with a carrier partner who can provide top notch integrated cyber services as well as the support of an experienced cyber claims team.

The real-life examples from our own claims database are varied; first-party cyber coverage and exposures can lead to large claims, and when we think of cyber events we tend to think of huge organizations. But sometimes it's the simplest little thing that can lead to a claim. Here are some examples of the kinds of claims our team has seen:

- An Ohio healthcare organization had to notify approximately 7,500 patients due to an employee accessing medical records without proper authorization. Patients in 9 states required notification and credit monitoring services. The Office of Civil Rights (OCR) made a request for additional information regarding this incident.
- An Arkansas medical center had to notify approximately 2,100 patients and employees after a home-health aide's home was burglarized. This incident warranted extra scrutiny from the OCR and a request for information was issued.
- A California healthcare organization had to notify approximately 1,000 patients when an A/R manager sent an erroneous email, that included patient medical records and reports, to an incorrect recipient.
- A California hospital had to notify approximately 6,000 individuals due to a breach of a business associate's systems. The BA operates the hospital's electronic medical record (EMR) system. OCR requested additional information about the incident.

State/federal regulations also factor into telehealth risk assessment

Much like regular healthcare coverage, there should also be certain coverages in every virtual care policy that would help the insured retain defense and respond in the event of a non-compliance inquiry. For those telehealth appointments that must be Health Insurance Portability and Accountability Act (HIPAA) federal or state compliant, this can be a complicated thing to track, as there are different cyber laws in virtually every state. One good resource is this interactive digital map, which provides detailed information on the state-by-state laws governing the provision of telehealth services across the US.

In some cases, laws have been relaxed due to COVID-19, but it remains to be seen if that will continue. Some regulatory changes that facilitated expanded use of telehealth have been made permanent (for example, the Centers for Medicare & Medicaid Services' expansion of reimbursable telehealth codes for the 2021 physician fee schedule), but others may return to pre-pandemic guidelines when the public health emergency expires, so it's important to watch closely.

Education and services are an essential part of comprehensive virtual care coverage

It's essential that brokers regularly talk about cyber-related risk with policy holders, who may be new to these exposures. Virtual care requires a thorough understanding of cyber and healthcare exposures which may go beyond the expertise of many broker specialists, so it's important to find an insurance partner with the education and service capabilities to fill this gap. Your insurance partner's cyber claims program should include an experienced team offering both breach resolution services and access to experts in the field to facilitate awareness and help insureds take necessary precautions.

For companies engaged in virtual care, now is the time to focus on your cybersecurity. Revisit technology choices that may have been made in haste during the pandemic, evaluate privacy rules and platforms, and ensure that you have the coverage in place to protect against all potential risk exposures. In addition, take the time to educate your employees on what cyber security looks like, and ensure you have guidelines in place for people who are accessing your networks remotely.

Looking to the future, we anticipate that telehealth models will move from purely "virtual urgent care" to encompass a wide range of services, solutions, and integrated care models. Proper due diligence during the underwriting review can help identify key technology and cyber exposures and aid brokers in guiding their clients through this new world.

Jennifer Schoenthal

Jennifer underwrites a wide range of risks found within the miscellaneous healthcare sector including categories such as healthcare staffing, home health, behavioral health, chemical detox, tissue/blood banks, organ procurement organizations, contract research organizations (CROs), correctional healthcare, medi-spas, occupational health, dialysis clinics, ground and air ambulances. Jennifer is the lead underwriter and global product leader of Beazley Virtual Care, a pioneering insurance policy that covers all organizations involved in the provision of telemedicine/telehealth.

jennifer.schoenthal@beazley.com
+1 770 351 1701

Dakai Pouncey

Dakai is an Assistant Claims Manager for Technology, Media and Business Services at Beazley. Dakai handles cyber claims on the Beazley Breach Response form.

dakai.pouncey@beazley.com
+1 212 801 7123