WEBINAR

TOP TAKEAWAYS

CYBERSECURITY & INSURANCE COVERAGE IN THE AGE OF TELEHEALTH: UNDERSTANDING & MITIGATING YOUR RISK

With more frequent and more severe ransomware attacks against health care platforms and vendors and the increasing use of telemedicine, it is critical to understand how to proactively defend your organization using robust legal, regulatory and cyber-coverage strategies. In this webinar, McDermott partners Dale Van Demark and Edward Zacharias joined Brett Buchanan of Marsh & McLennan Agency and Larry Hansard of Gallagher USA to explore the intersection of telemedicine and cybersecurity. Our panelists offered attendees a road map for navigating this rapidly changing space, including practical strategies for shoring up their defenses and addressing potential risks to their businesses. Read on for select highlights from this insightful discussion, and click here to view the full webinar.

1

Providers engaging in telemedicine should consider **three critical areas of insurance coverage**: medical professional liability, technology errors and omissions, and cyber/privacy liability. “Several carriers have packaged these three important coverages into a one-policy format, referred to as a virtual health program,” Hansard said.

2

A medical professional liability program should include incident reporting, punitive damages, and sexual abuse and molestation. The latter may seem surprising in a telemedicine context, but is important given reports of inappropriate patient behavior during telemedicine encounters, Hansard said.

3

New telehealth technologies, such as AI chatbots for patient intake, create new and more complex bodily injury exposures, Buchanan said. “**Working with an insurance underwriter that understands these nuances is absolutely key**,” he said. In addition to bodily injury, coverage should include technology errors and omissions, cyber liability and general liability.

4. With the explosion of investment in telehealth has come an increase in cyber threats targeting telehealth. **Ransomware attacks in particular are on the rise**, often deployed via email phishing scams. “The most effective means of trying to avoid these issues is a personnel issue and a training issue, and making sure folks are aware of how to spot the common factors in phishing emails and scams that could lead to ransomware or other malware,” Zacharias said.

5. In this environment of increasing cyber risk, **a proactive incident response plan is more critical than ever**. Such a plan should include the following elements: preparation, detection, containment, eradication, recovery and post-event analysis. The latter step, plus any necessary action items based on lessons learned, is important to help prevent similar events in the future.

6. **Most telemedicine and digital health companies are underinsured for cyber liability,** and the costs for such coverage are rising steeply. This situation raises the question of how much coverage is sufficient. The answer depends on the provider organization, the types of activities in which it’s engaged, and the number of health records it has, Zacharias says. “Balancing the organization’s resources with its risk profile has become increasingly challenging,” he said. “I don’t know that there’s a one-size-fits-all right answer, but it’s something that providers need to be focused on.”

VISIT **MWE.COM/HEALTH**

McDermott
Will & Emery