Cybersecurity – Long-Term Care Facilities in the Crosshairs

By Thomas J. DeMayo, Principal, Cyber Risk Management

Over the years, we have worked with many long-term care facilities and have direct experience with how long-term care facilities typically safeguard the electronic protected health information (ePHI) of the residents they serve. What we often find is that long-term care providers are struggling with understanding their cyber exposure and managing their cyber risk. We fully understand the challenge. Long-term care facilities typically do not have sufficient internal IT resources, most of which are outsourced to a third party managed service provider, and may not have the funds readily available as a result of continued care reimbursement rate decreases.

Risky Business

While we understand the challenges, without question long-term care providers are — and will be — targeted by cyber criminals. It is only a matter of time before a major cyber breach occurs that will thrust long-term care providers into the headlines.

The Health Insurance Portability and Accountability Act (HIPAA) requires the protection of ePHI from any anticipated threat, inclusive of cyber threats. Should the ePHI be breached and regulators identify that the facility turned a blind eye to cybersecurity or did not take the time to identify cyber risk and reduce it to acceptable levels, monetary penalties in the millions could result.

We often are asked the question: "What information would cyber criminals want from us?" While most facilities believe the answer is "nothing," what many are not fully aware of is that they possess what cyber criminals perceive to be the most valuable information on the black market — medical records. Medical records not only facilitate identity theft, but they also could grant access to insurance fraud and prescription medications. Medical records can be sold for 10 times the value of a single social security number. Further, as an added bonus to cyber criminals, long-term care facilities often manage resident funds, having the necessary information to target and deplete resident bank accounts.

In the Breach

Ransomware, the malware that encrypts data and holds the network hostage, has made it more pressing than ever for long-term care providers to assess and manage their cybersecurity risk. The U.S. Department of Health and Human Services (HHS) has made it clear that ransomware that touches patient data is to be considered a breach and is to trigger a breach notification risk assessment and response.

Such a breach may result in the formal and comprehensive investigation of the HIPAA compliance of the facility by HHS, notification to news outlets, fees associated with computer forensic incident response, resident credit monitoring, remediation expenses, and monetary penalties directly proportional to the extent that HHS concludes that the long-term care facility was negligent in the cyber protections of ePHI. Such ramifications could destroy the business.

Managing Cyber Risk

While it seems overwhelming, a long-term care facility should be doing the following to proactively manage their compliance and cyber risk:

1. Disregard the notion that cyber criminals will not target a long-term care facility. They will, and are, targeting your facility as you read this article.
2. Do not blindly assume that your IT department or managed service provider has cybersecurity and HIPAA compliance under control.
3. Put cybersecurity on your board's agenda. Boards of long-term care facilities have a fiduciary responsibility to ensure that both HIPAA and cyber risk are being addressed and managed to acceptable levels.
4. Make sure the board and management of the facility fully understand the long-term care HIPAA requirements as they relate to the security of ePHI and can demonstrate compliance with the HIPAA requirements. While it sounds straight forward, the HIPAA security rule has 70+ standards that need to be addressed, many of which are subjective and may require consultative input to ensure reasonableness based on the facility's IT circumstances.
5. Have independent HIPAA compliance and cybersecurity assessments to ensure that the facility is appropriately managing their regulatory and cyber risk. Independent assessments are critical in ensuring that senior management and the board have objective insight into the sufficiency of the HIPAA compliance and cybersecurity risk management strategy.
6. Shift your view of cybersecurity and HIPAA compliance from that of a business expense to that of a required and necessary business enabler. For a long-term care facility to continue to meet its mission of providing quality care, it needs to embrace information security controls as a necessary component of providing that care

No Quick Fix

It is easy to assume that IT can and should implement a single solution to address and remediate all compliance and cyber risk. For the foreseeable future, no such solution exists.

A long-term care facility must implement controls across the people, processes and technology that support and manage their day-to-day operations. This requires the implementation of a comprehensive and holistic strategy to address IT compliance and cyber risk at each risk layer of the facility, both technical and non-technical. While this sounds expensive, it doesn't have to be. Many long-term care facilities have the foundation of what they need to establish a reasonable cyber program, they just need assistance in how to leverage it more effectively.

Contact Us

If you have any questions on how to address the compliance and cyber risk within your long-term care facility, please contact Tom DeMayo, Principal at tdemayo@pkfod.com or Chris McCarthy, Partner at cmccarthy@pkfod.com.

www.pkfod.com

About PKF O'Connor Davies

PKF O'Connor Davies, LLP is a full-service certified public accounting and advisory firm with a long history of serving clients both domestically and internationally. With roots tracing to 1891, nine offices in New York, New Jersey, Connecticut and Maryland, and more than 700 professionals, the Firm provides a complete range of accounting, auditing, tax and management advisory services. PKF O'Connor Davies is ranked 28th on *Accounting Today's* 2017 "Top 100 Firms" list and is recognized as one of the "Top 10 Fastest-Growing Firms." PKF O'Connor Davies is also recognized as a "Leader in Audit and Accounting" and is ranked among the "Top Firms in the Mid-Atlantic," by *Accounting Today.* In 2017, PKF O'Connor Davies was named one of the 50 best accounting employers to work for in North America, by *Vault*.

PKF O'Connor Davies is the lead North American representative in PKF International, a global network of legally independent accounting and advisory firms located in over 400 locations, in 150 countries around the world.