02/08/19

Cyber Risk Exposure for Long Term Care Facilities

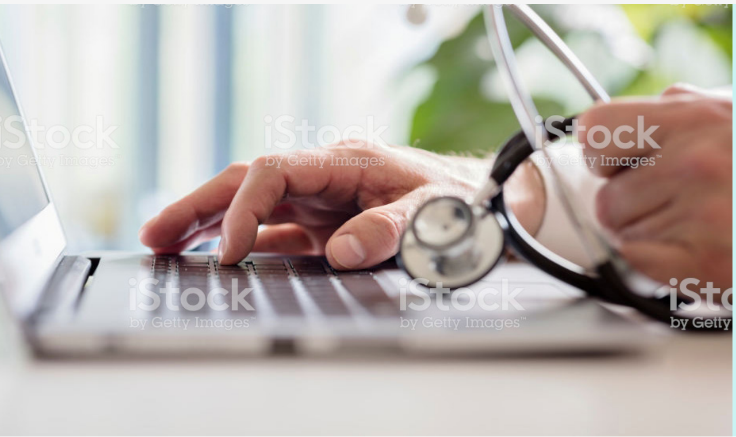
Katie Wagner and Daniel Frusciano

As technology continues to advance, long term care providers, like other healthcare providers, have become increasingly driven by digital data. Electronic storage of residents' medical records and the virtual delivery of care have made it imperative for management to protect sensitive data. The challenge is that many nursing homes and other senior or assisted living facilities (collectively "Long Term Care providers") may not have a response plan in place to shield themselves and their patients/residents in the event of a cyber attack. Resultant potential for significant financial losses related to recovery and remediation could be significant.

Exposure to cyber attacks can impact every segment of the healthcare sector. Long Term Care providers, however, are particularly vulnerable given the nature of on-site adult living and the manner by which patient health information is managed and delivered. According to a report by the Leading Age Center for Aging Services Technologies (CAST), most small to mid-size institutions are at greater risk than traditional healthcare organizations because those facilities may be less mature in the deployment of cybersecurity plans for resident/patient protection. The most predominant threats facing Long Term Care providers arise from increased reliance on Electronic Health Records (EHR) and care management via Telehealth platforms.

Innovative EHR technology allows physicians, hospital systems and other healthcare facilities to maintain and store data and share personal clinical treatment electronically. EHR files can include everything from patient demographics, prescriptions, procedures, test results, and much more. The overarching advantages of EHRs have led to improved patient care and greater delivery efficiencies for the healthcare provider. Yet, cyber attacks within the healthcare universe are unfortunately inevitable. Trends suggest that "25 million people or one out of every 13 patients will have their medical or personal information stolen from their healthcare facility's digital records between 2015 and 2019," as reported by Healthcare IT News.

Telehealth platforms present new challenges for the protection of an individual's medical information. More than 20 million Americans now benefit from some manner of remote health care treatment. Various factors drive the need for telemedicine care, serving people living in isolated or rural areas of the country that may not have ready access to receive needed healthcare services. The demographic most aided by telemedicine care is the growing number of elderly Americans. Long Term Care providers are relying on patient video conferencing, electronic sharing of an individual's medical condition, and remote diagnosis to deliver professional patient/resident care.



In the event of a cyber breach, the monetary costs involved with remediation of the network, notification expenses and any damages incurred by a resident, especially where the facility has been deemed negligent in safeguarding medical records, can be staggering. Long Term Care providers should have a cyber risk response plan in place. In addition, they should carry cyber liability insurance that provides firstand third-party coverage for the loss of or damage to digital data.

Small to mid-size Long Term Care providers are not immune to cyber-attacks. Securing comprehensive facility-wide incident liability coverage that protects against a potential network security and privacy breach can be a daunting undertaking. And due to the potential for coverage overlap or coverage conflict, it is important for providers to obtain a cyber liability policy that coordinates with their healthcare professional and general liability policy.

IronHealth in collaboration with its affiliate, IronPro, has developed an insurance solution that includes comprehensive coverage for cyber security and privacy liability risks on its long term care professional and general liability policy. For nearly any risk underwritten by IronHealth and in a single and seamless transaction, an endorsement can be added that provides IronPro's specialized coverage directly to the IronHealth policy. The endorsement extends protection against network security and privacy liability risks with reimbursement of costs associated with breach notification, recovery and remediation, any regulatory fines, and digital asset expenses, as well as business interruption income loss, with dedicated limits of up to $1 million. Insureds and brokers benefit from working with one underwriting team and one integrated claims process to avoid conflicts of interest and avoid any disconnected coverage disputes amongst several parties.

Long Term Care providers require diligent pursuit of effective actions for adaption of cyber security plans that set forth processes and procedures to detect and execute a coordinated response. Heightened awareness of potential exposure amongst the facility's management, staff and healthcare providers is an essential first step. Precautionary measures and informed recognition of cyber security threats to residents and patients can lay the foundation for a sound risk management strategy for long term care facilities.

** The terms telehealth and telemedicine are often used interchangeably. In general, telemedicine is considered the clinical application of technology, while telehealth encompasses a broader, consumer-facing approach.*

Please visit *ironshore.com* for all disclaimers.