May 5, 2016 Publication

Increased Ransomware Attacks and Phase 2 HIPAA Audits: Two Closely-Related Issues for Long Term Care Providers

Lane Powell White Paper

Long Term Care Provider Data Targeted and Held Hostage by Malicious Software

Long Term Care (LTC) facilities are increasingly targeted by criminals who seek to profit by infecting LTC computer systems with ransomware. Ransomware is a type of software that restricts access to infected computer systems by encrypting data, even across multiple servers. It can be impossible to decrypt those files without the encryption key. Criminals then demand payment of a ransom in exchange for the encryption key.

Why Target LTC Providers?

Ransomware and other types of cyber-attacks on LTC and other health care providers are likely increasing for at least two reasons. First, providers may be viewed as soft targets without robust computer system security or backup systems. Second, because of the private nature of the protected health information contained in providers' computer systems, providers may be viewed as more willing to promptly pay whoever is holding the files containing that information hostage.

Notification and Publicity

HIPAA may require covered entities and their business associates to provide notification following a breach of unsecured protected health information. A breach is a defined term, constituting an impermissible use or disclosure of covered information that compromises the security or privacy of the protected health information (PHI). In the case of ransomware, which can sometimes lock up PHI without any evidence that the PHI was used or disclosed, an entity's HIPAA notification obligations must be analyzed on a case-by-case basis. Regardless of whether a particular ransomware incident requires notification, the incident can create public relations problems for health care providers. The first half of this year has brought with it an increasing wave of ransomware incidents

Topics

Privacy & Data Security

Senior Living & Long Term Care

Related People

Related Practices & Industries

Privacy & Data Security

Senior Living & Long Term Care

that have been widely reported and scrutinized. It was reported that in February, a ransomware called "Locky" infected Hollywood Presbyterian Medical Center in Los Angeles, which took computers offline for a week, and the next month, the same strain of ransomware infected Methodist Hospital in Henderson, Kentucky.

What Now?

While the ransomware threat is increasing, there are steps LTC providers should take to help deal with that threat.

- Assessment: HIPAA requires covered LTC providers to conduct a risk analysis and to implement a risk management program. This means covered entities must implement a risk management program that, among other things, identifies ePHI data usage and systems; identify gaps (or potential gaps) in compliance; implement and constantly review data breach response plans; determine whether the covered entity (and its vendors and business associates) are adequately insured to cover risks associated with cyber-attacks; and train employees on security awareness. As part of the assessment, covered entities should also identify a data breach response team.
- Review: HIPAA also requires covered entities to regularly review data security policies and procedures and to make appropriate changes.
- Document Efforts: Make sure to document all the steps you take to comply with HIPAA and to prepare for a ransomware/data breach incident.

Phase 2 HIPAA Audits Underway

The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) has begun Phase 2 of its efforts to assess compliance with the HIPAA Privacy, Security and Breach Notification Rules. According to OCR, it will use the information obtained from the audits to develop tools and guidance to help covered entities with self-evaluation compliance and breach prevention.

OCR launched Phase 1 in 2011 as a pilot program, which involved an evaluation of certain covered entities to determine HIPAA compliance (or lack thereof). Now, with its Phase 2 audit program, OCR will go further, reviewing policies and procedures adopted and employed by covered entities and their business associates to comply with the Privacy, Security and Breach Notification Rules. Phase 2 begins with OCR sending emails to covered entities and business associates requesting verification of addresses and contact information. HHS has cautioned that "communications from OCR will be sent via email and may be incorrectly

classified as spam" and it expects "entities to check their junk or spam email folder for emails from OCR." If you receive such an email, respond promptly. OCR has also made available a sample of its initial Phase 2 automated communication, which can be found at here.

As Phase 2 progresses, OCR will send covered entities a pre-audit questionnaire. The questionnaire will seek data about the size, type and operations of covered entities. OCR will use that, and other data, to help create groups of potential auditees. In advance of receiving the questionnaire, you should update your list that includes the identity of your business associates and their contact information. Every covered entity and business associate is eligible for an audit.

Next, OCR will conduct two rounds of "desk audits," which it plans to complete by the end of 2016. The desk audits will focus on compliance with specific requirements of the Privacy, Security and Breach Notification Rules. As part of that process, OCR will send auditees a request for specific documents related to the entities' implementation and compliance with these rules. OCR may decide to not consider documents that were prepared only after the audit process began. Accordingly, covered entities that have not already prepared implementation and compliance documents should do so immediately.

OCR will then launch a third set of Phase 2 audits, which will be onsite, each lasting three to five days in length. The onsite audits will be fewer in number than the desk audits, and they are expected to examine a broader scope of requirements from the HIPAA Rules than will the desk audits. Some desk auditees may be subject to a subsequent onsite audit as well.

OCR auditors will review information and documentation provided by audited entities. Entities that are subject to either a desk or onsite audit will have 10 business days to submit written comments and responses to the draft findings, and those responses will be included in a final audit report. It is critical that covered entities begin preparing now for possible inclusion in the group of desk or onsite audits. If an audit report indicates a serious compliance issue, OCR may initiate a compliance review to further investigate. Keep in mind that under the Freedom of Information Act (FOIA), OCR may be required to release audit information in response to public requests. This could have long-term reputational consequences to audited covered entities. In addition, OCR has been increasingly active in addressing data breach violations, including a recent $850,000 settlement related to the theft of an unencrypted laptop containing ePHI.