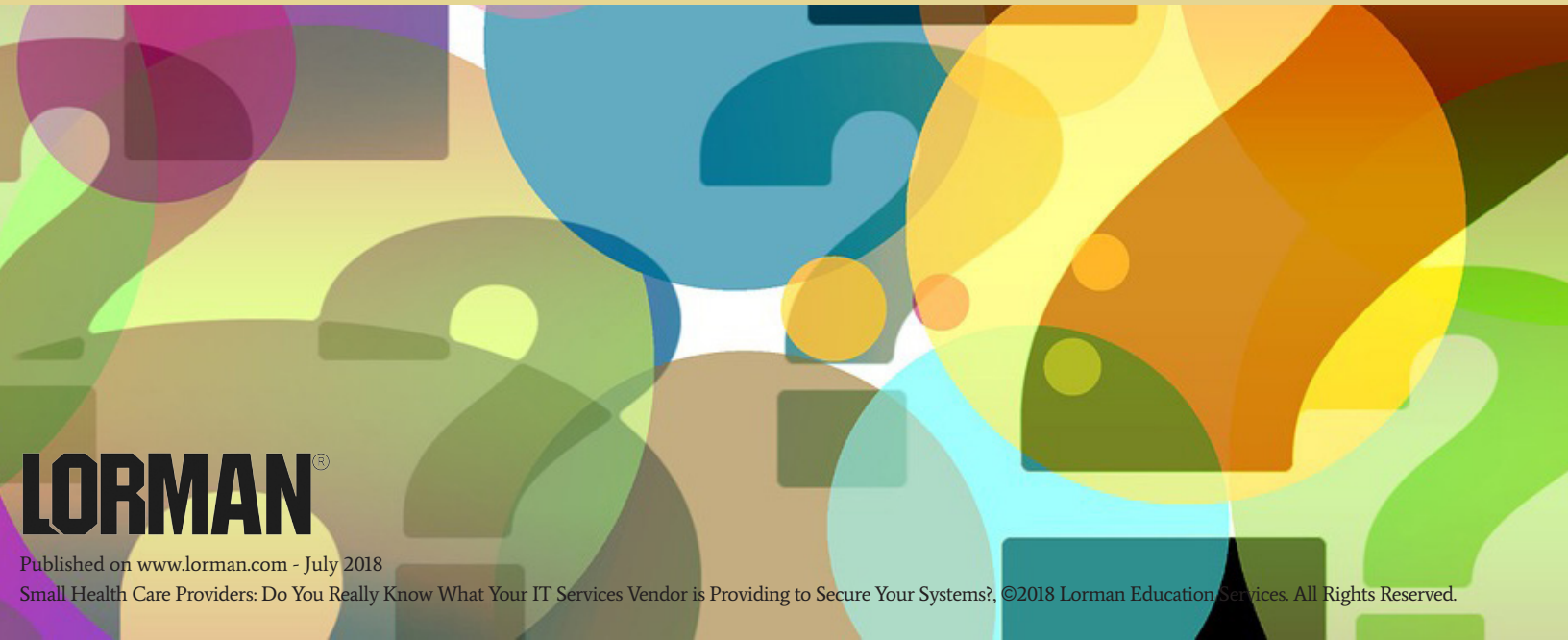
Small Health Care Providers: Do You Really Know What Your IT Services Vendor is Providing to Secure Your Systems?

Prepared by:
Paulette Thomas
Baker & Hostetler LLP



LORMAN®

Published on www.lorman.com - July 2018

INTRODUCING

Lorman's New Approach to Continuing Education

ALL-ACCESS PASS

The All-Access Pass grants you UNLIMITED access to Lorman's ever-growing library of training resources:

- ☑ **Unlimited Live Webinars** - 120 live webinars added every month
- ☑ **Unlimited OnDemand and MP3 Downloads** - Over 1,500 courses available
- ☑ **Videos -** More than 1300 available
- ☑ **Slide Decks -** More than 2300 available
- ☑ White Papers
- ☑ Reports
- ☑ Articles
- ☑ ... and much more!

Join the thousands of other pass-holders that have already trusted us for their professional development by choosing the All-Access Pass.

Get Your All-Access Pass Today!

SAVE 20%

Learn more: www.lorman.com/pass/?s=special20

Use Discount Code Q7014393 and Priority Code 18536 to receive the 20% AAP discount.

*Discount cannot be combined with any other discounts.

Small Health Care Providers: Do you really know what your IT services vendor is providing to secure your systems?

*Written by **Paulette Thomas** on December 27, 2017*

A small health care provider such as a physician office or clinic often will contract with an IT services vendor to meet overall IT needs to operate the business. A small health care provider may not have the resources and expertise to understand the technical support that an IT services vendor provides, and it relies upon the IT services vendor's expertise to support, secure, and protect the IT systems and patient data. A health care provider that is a covered entity as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is required to comply with HIPAA, the Health Information Technology for Economic and Clinical Health Act (the HITECH Act), and the privacy and security regulations promulgated (the Privacy and Security Rules). HIPAA requires a covered entity to enter into a business associate agreement with an IT services vendor that has access to, uses, maintains, and transmits protected health information (PHI) on behalf of the health care provider. The business associate agreement includes the regulatory minimum requirements that the business associate must take to protect the covered entity's PHI. But does the health care provider

understand what the IT services vendor is providing to secure PHI from unauthorized use and disclosure?

The U. S. Department of Health and Human Services Office for Civil Rights (OCR) issued guidance in October 2016, on HIPAA compliance when a covered entity and a business associate utilize cloud solutions for data management. The guidance, while focusing on cloud services, also easily applies to procuring and using traditional IT services. The parties should specify in the IT services agreement which party will be responsible for implementing the Privacy and Security Rules' administrative, physical, and technical safeguards. Both parties should conduct a security risk analysis to identify the potential threats to and vulnerabilities of the confidentiality, integrity, and availability of the health care provider's electronic PHI. For the small health care provider, this may require engaging the expertise of an IT security firm to conduct the security risk analysis and to develop the risk management plan. Although an additional expense, obtaining a security risk analysis will go a long way to help the health care provider determine where security is needed to protect patient information, and demonstrate compliance with the HIPAA Privacy and Security Rules if OCR were to investigate a breach.

In the Guidance, OCR sets forth recommendations for parties to consider when entering into a services agreement that are applicable to traditional IT services:

- The IT services agreement sets forth the respective parties' responsibility to secure the information system consistent with the HIPAA Privacy and Security Rules, such as:
    - User tools that may be used to increase privacy and security protections.
    - Backup and data recovery to respond to emergency situations such as ransomware and other malware attacks.
    - The manner in which the IT services provider will return data to the health care provider or securely destroy the data after the services are terminated.
    - Delineation of responsibility between the parties for implementation and management of the IT security services.
    - Use, retention, and disclosure limitations.
    - Use of encryption.
    - Responsibility for access and termination controls.
    - Breach and security incident monitoring and notification,
    - Cyberliability insurance requirements.
    - Documentation and data retention requirements in the event of a breach, such as preservation of logs and equipment, to demonstrate compliance with the HIPAA Privacy and Security Rules and state law requirements.

    - Cooperation and assistance in investigating a breach, security incident, and OCR investigations.
    - Requiring the IT services vendor to provide documentation of its privacy and security practices, such as submitting to a security audit.
    - Data and log retention requirements.
- The health care provider and the IT services vendor are required to enter into a HIPAA-compliant business associate agreement, and should review the terms set forth in the service level agreement for consistency with the parties' regulatory obligations under the business associate agreement.
- The health care provider and the IT services vendor should conduct a security risk analysis to identify gaps in the services and implement a risk management plan to address the identified risks and allocate responsibility for compliance.

In the publication, "Health Information Privacy in the Digital Age," OCR indicates that the agency will continue to focus enforcement efforts and resources on matters that identify industrywide noncompliance, where corrective action under HIPAA may be the only remedy, and where corrective action benefits the greatest number of individuals. OCR reminds covered entities and business associates of their ongoing HIPAA responsibilities, and OCR has indicated that it will review the contractual obligations between the respective parties regarding control and implementation of the security features of the

[cloud] services consistent with the HIPAA Security Rule when investigating any breach involving such parties. Expect OCR to use this same approach when evaluating the respective parties' obligations under traditional IT services in the event of an investigation of a health care provider following a breach of unsecured PHI involving contracted IT vendor services.