HIPAA PHASE 2 AUDITS ARE HERE. ARE BUSINESS ASSOCIATES READY?

SEPTEMBER 2016

The United States Department of Health and Human Services (“HHS”) Office for Civil Rights (“OCR”) has begun Phase 2 of its audit program. Phase 2 will address both Covered Entity and Business Associate compliance with the Privacy, Security, and Breach Notification Rules of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). Phase 2, which follows OCR’s initial Phase 1 Pilot audits of 115 Covered Entities in 2011 and 2012, further continues OCR’s effort to conduct periodic compliance audits, mandated by HIPAA, as amended by the Health Information Technology for Economic and Clinical Health Act (“HITECH”) and the HIPAA Omnibus Final Rule (“Omnibus”). OCR has announced that it is considering a broad spectrum of audit candidates to better assess HIPAA compliance across the health care industry. The Phase 2 audits seek to enhance industry awareness of compliance obligations. Based on the information obtained in the Phase 2 audits, OCR plans to develop tools and guidance to assist the industry in compliance self-evaluation and in preventing breaches. The results will be used to develop OCR’s permanent audit program.

What does this mean for the myriad of businesses who work with Covered Entities, such as health care providers, insurers, and many employee-sponsored group health plans? It means those businesses now need to prepare for HIPAA audits in the same way that Covered Entities do. This need to prepare applies equally to subcontractors of Business Associates who may not have direct contact with the Covered Entity. Equally important, it means that many businesses, who have historically not recognized that they qualify as Business Associates or who have proactively avoided signing Business Associate Agreements and argued that they are not Business Associates, will be subject to HIPAA requirements and the concomitant liability for failure to comply.

DO YOU KNOW IF YOU ARE A BUSINESS ASSOCIATE?

Generally, a Business Associate is a person or entity that performs certain functions or provides certain services for a Covered Entity involving the use or disclosure of protected health information (“PHI”). Omnibus both clarified the definition of Business Associate as including those entities that create, receive, maintain, or transmit PHI on behalf of a Covered Entity and expanded it to include patient safety organizations, health information organizations, E-prescribing gateways, and other entities that provide data transmission services to a Covered Entity and require routine access to PHI, as well as personal health record vendors. As a result, many IT consultants, software vendors, and cloud service providers who historically argued against being a Business Associate find themselves clearly meeting the definition. Additionally, after Omnibus, a subcontractor that creates, receives, maintains, or transmits PHI on behalf of a Business Associate also falls within the regulatory definition of Business Associate. Many businesses have not yet come to grips with the stark reality that they are subject to HIPAA as a Business Associate despite the fact that after the Omnibus compliance date (September 23, 2013), status as a Business Associate no longer depends on the existence of a Business Associate Agreement (“BAA”). If you have not acknowledged or recognized that you are a Business Associate, then in all likelihood you do not have a BAA in place. That is your first point of non-compliance, and it can subject you and the Covered Entity(ies) with whom you work to penalties for not having an agreement in place.
PREPARING FOR AN OCR AUDIT TO ENSURE HIPAA COMPLIANCE

If OCR determines that you meet the definition of a Business Associate, then it can and will hold you accountable for compliance. Every Business Associate is eligible to be audited. Many entities have yet to complete some of the basic tasks required by HIPAA. For example, the HIPAA Security Rule requires, among other things, that Covered Entities and Business Associates have a security management process that includes an accurate and thorough risk assessment, a risk management program, a sanctions policy, and a review of information system activity. Business Associates are now directly liable for HIPAA compliance, and their obligations are not dependent on the existence or terms of a BAA. HIPAA still requires that Covered Entities obtain written assurances from their Business Associates that those Business Associates will protect the privacy and security of PHI; however, liability attaches regardless of the terms of the BAA or even if there is no BAA at all. This creates another area of focus for Business Associates. The terms of the BAA may add compliance requirements for the Business Associate that go beyond what HIPAA requires.

As for the audit process, in May 2016, OCR sent pre-audit questionnaires to a large group of Covered Entities, and on July 11, 2016 it notified 167 Covered Entities that they had been selected for the initial round of Phase 2 audits. The pre-audit questionnaires sought to gather information about the type, size, and operations of each Covered Entity. The Covered Entities selected for an audit will be sent a second email requesting a list of the Covered Entity’s Business Associates. The audit letter will include document requests related to the topics selected for that particular audit. The auditee will have 10 days to respond to the document requests and will be required to submit the response electronically through the OCR website. This short time frame makes it imperative that Business Associates take the steps necessary for HIPAA compliance long before the receipt of an audit letter. The compliance process is not static. It requires organizations to vigilantly monitor their programs, audit their programs, and make changes based on what is learned from the self-audits. Failure to comply can have significant consequences. Civil monetary penalties can range from $100 to $50,000 per violation (or per record) and can total up to $1.5 million per type of violation, per calendar year – not to mention the damage to business reputation and potential criminal penalties.

Many businesses are not prepared because they have not undertaken the necessary steps to comply with the HIPAA Privacy, Security, or Breach Notification Rules. Are you at risk?

ADDITIONAL INFORMATION

For more information about the audit protocol and preparing for a potential audit or the definition of a Business Associate or Business Associate Agreements, please contact:

- **JOSEPH DICKINSON** | 216.696.4569 | joseph.dickinson@tuckerellis.com
- **WILLIAM BERGLUND** | 216.696.2698 | william.berglund@tuckerellis.com
- **EDWARD TABER** | 216.696.2365 | edward.taber@tuckerellis.com

This Client Alert has been prepared by Tucker Ellis LLP for the use of our clients. Although prepared by professionals, it should not be used as a substitute for legal counseling in specific situations. Readers should not act upon the information contained herein without professional guidance.

© 2016 Tucker Ellis LLP. All rights reserved.