THE OCR'S PHASE 2 HIPAA AUDIT PROGRAM AND CLOUD-SERVICE PROVIDERS, AND AN ALERT REGARDING PHASE 2 AUDIT EMAIL PHISHING SCAMS

November 29, 2016

By: Gavin C. Gaukroger

The U.S. Department of Health & Human Services (HHS) Office for Civil Rights (OCR) is undertaking continued efforts to assess compliance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security and Breach Notification Rules, and auditing "covered entities" (health care providers, health plans, and health care clearinghouses) and "business associates" (discussed herein) to determine whether protected health information (PHI) is in fact protected. The HIPAA Rules are intended to protect individuals' health care privacy rights and secure medical data from unauthorized disclosure. The OCR's Phase 2 HIPAA Audit Program, unlike the Phase 1 pilot audit program conducted in 2011 and 2012, includes OCR audits of companies operating as business associates to covered entities.

A "business associate" is an entity or person, other than a member of the workforce of a covered entity, that performs functions or activities on behalf of, or provides certain services to, a covered entity that involve creating, receiving, maintaining, or transmitting PHI. A business associate also is any subcontractor that creates, receives, maintains, or transmits PHI on behalf of another business associate. The HHS has given guidance that "a data storage company that has access to protected health information (whether digital or hard copy) qualifies as a business associate, even if the entity does not view the information or only does so on a random or infrequent basis." This includes datacenters, server farms, remote application services providers, and other hardware or software systems providers which can store patient data, including cloud-service providers.

Notably, when a business associate subcontracts with another service provider, such a cloud-service provider to create, receive, maintain, or transmit ePHI on its behalf, the cloud-service provider is also viewed as a business associate of the business associate. As a result, the covered entity (or business associate) and the cloud-service provider must enter into a HIPAA-compliant business associate agreement. With only narrow exception, a cloud-service provider is also directly liable for compliance with the applicable requirements of the HIPAA Privacy, Security and Breach Notification Rules and thus should become or remain compliant. A narrow exception applies for a "conduit" of PHI and ePHI. HIPAA defines a conduit as a business that simply passes PHI and ePHI through their system, like the USPS, FedEx, UPS, phone companies and Internet Service Providers that simply transport data and do not store it. P*ersistence* of storage is the qualifier that determines whether a business is a business associate or a conduit of PHI. Cloud-based systems, which traditionally were conduits of information, now often "maintain" files of the information transmitted through their channels and thus are not mere conduit businesses.

If your company serves as a business associate to a covered entity or relies on subcontractors to store PHI or ePHI data for your business or your clients' businesses, each must be HIPAA compliant and contractually bound by HIPAA-compliant business associate agreements. Contact Gavin Gaukroger for more information about the HIPAA Rules and your company's compliance.

Alert Regarding Phishing Scams:

According to the HHS, covered entities received Phase 2 Audit notification letters in July, 2016 and business associates were to receive notification letters in "the fall" of 2016. The HHS has issued guidance about the manner in which business associates are being contacted for the pre-audit communications from the OCR: "Communications from OCR will be sent via email and may be incorrectly classified as spam. If your entity's spam filtering and virus protection are automatically enabled, we expect you to check your junk or spam email folder for emails from OCR."

As an apparent result of the e-mail communication method chosen by the OCR to issue pre-audit and audit notifications, on November 28, 2016, the HHS issued the "Audit Phase 2" Alert below and displayed on the HHS's website here:

Audit Phase 2

Alert: Phishing Email Disguised as Official OCR Audit Communication – November 28, 2016

It has come to our attention that a phishing email is being circulated on mock HHS Departmental letterhead under the signature of OCR's Director, Jocelyn Samuels. This email appears to be an official government communication, and targets employees of HIPAA covered entities and their business associates. The email prompts recipients to click a link regarding possible inclusion in the HIPAA Privacy, Security, and Breach Rules Audit Program. The link directs individuals to a non-governmental website marketing a firm's cybersecurity services. In no way is this firm associated with the U.S. Department of Health and Human Services or the Office for Civil Rights. We take the unauthorized use of this material by this firm very seriously. In the event that you or your organization has a question as to whether it has received an official communication from our agency regarding a HIPAA audit, please contact us via email atOSOCRAudit@hhs.gov.

All covered entities and business associates should anticipate being on the "list" of companies served with pre-audit or audit notifications from the OCR and take HIPAA compliance seriously. It is virtually a weekly, if not daily, occurrence that a major fine is levied against a company for unauthorized disclosures of PHI. Companies which are victims of hackers, thieves, or even innocent employee negligence are all subject to enforcement actions by the OCR. The best protection is planning. Attorneys at Berger Singerman are experienced in crafting business associate agreements, HIPAA compliance policies, and, if necessary, guiding their clients through the data breach notification procedures of HIPAA and related state data breach notification laws.

For more information on this topic, please contact the author, Gavin Gaukroger, on the firm's Dispute Resolution Team.

Related Team Member(s)

Gavin C. Gaukroger