COMPLIANCE ALERT

April 2018

# Are you Prepared for a HIPAA Audit?

The Health Insurance Portability and Accountability Act (HIPAA) protects the privacy and security of an individual's protected health information (PHI) by governing how covered entities use, store, and share health information. As covered entities under HIPAA, self-funded plan sponsors must comply with HIPAA's Privacy, Security, and Breach Notification Rules. The Department of Health and Human Services Office of Civil Rights (OCR) is required to conduct periodic audits to ensure covered entity compliance.

The scope of OCR's multiphase audit program is limited to the Privacy, Security, and Breach Notification Rules. The primary purpose of the audits is to review how covered entities apply practical means of compliance and to uncover vulnerabilities that may not have been previously identified through other audits or individual complaints. With the information gathered, HHS intends to identify best practices and provide guidance for compliance issues that are found to need further clarity. However, if the OCR discovers a serious compliance issue, intentional non-compliance, or a lack of cooperation in addressing compliance shortcomings identified during the audit, the covered entity may be subject to a more comprehensive compliance review and penalties.

In some cases, the covered entity selected for audit may have only ten days and one opportunity to provide the OCR with documentation of compliance policies, procedures, and day-to-day practices. Therefore, it is in covered entities' best interests to prepare for a successful audit in advance. Foster & Foster recommends that self-funded plan sponsors prepare now by taking the time to shore up their PHI privacy and security practices as well as compile the documentation necessary to demonstrate their compliance efforts. Below is a checklist to help you get started:

## The Basics

- ❑ Name and title of the plan's privacy officer, security officer, and contact person(s)
- ❑ The plan's Notice of Privacy Practices and proof of distribution
- ❑ Plan documents and plan sponsor's certification of any plan amendments
- ❑ Copies of all business associate agreements

## Infrastructure

- ❑ Controls on physical access to electronic information systems and the facilities in which they are housed
- ❑ Contingency and backup plans, as well as procedures for emergency access to information systems containing electronic PHI
- ❑ Documentation regarding monitoring of systems and networks, including a listing of all network perimeter devices (e.g., firewalls and routers)

*(continued on next page)*

## Foster & Foster is Here to Help

**Foster & Foster works with employers to customize health care cost control strategies, and then successfully communicate, manage, and measure them. For guidance with regulatory compliance, contact Janet Stebbins, Compliance Consultant, at janet.stebbins@foster-foster.com.**

## Personnel

- ❑ The names and/or titles of the employees authorized to access the group health plan's PHI and for what purposes (i.e., plan administration)
- ❑ Procedures for the establishment and termination of users' access to computers storing electronic PHI
- ❑ Policies and procedures relating to workforce members' access to PHI via portable electronic devices and from non-worksite locations
- ❑ Documentation of HIPAA training for all employees with access to PHI (including dates and attendance records for training programs, training materials, and evidence that the training materials correspond to the plan's policies and procedures)
- ❑ Documentation of disciplinary actions or sanctions imposed on any workforce members who have violated HIPAA's privacy and security provisions
- ❑ The plan's breach notification procedures and documentation of any HIPAA complaints filed with the plan, along with the plan's investigation and resolution of the complaints (e.g., a complaint log)

## Risk Analysis and Management

- ❑ Risk analyses and risk management assessments relating to electronic PHI and compliance with the HIPAA security rule's standards and implementation specifications
- ❑ Procedures to audit information systems that contain or use electronic PHI, documentation of the audits conducted, and resolution of issues raised in such internal audits
- ❑ Documentation of prevention, detection, containment, and correction of internal security violations (incident reports and resolutions)
- ❑ Information regarding controls on Internet or other remote access activity, such as information on network infrastructure, platform, access servers, authentication, and encryption software
- ❑ Other information to document or substantiate implementation and maintenance of the administrative, physical, and technical safeguards required by the HIPAA security rule

## Individual's Rights

- ❑ Documentation relating to the plan's compliance with individual rights relating to PHI (for example, the plan's procedures and forms for requesting access to PHI, amendment of incorrect or incomplete PHI, an accounting of disclosures of PHI, and alternative communications or additional privacy protections for PHI)
- ❑ Logs of any PHI requests received, including the plan's response to each request

### Resources for More Information

For more information on the OCR HIPAA Audit Program, please visit:
**https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html#**

For more information on HIPAA and cyber security, please visit:
**https://www.healthit.gov/providers-professionals/guide-privacy-and-security-electronic-health-information**