HIPAA Audits to Increase in 2016

Martin Haitz | (484) 270-2575 | martin.haitz@marcumfs.com

Issued date: 04/18/16

On March 21, 2016, Health and Human Service's Office for Civil Rights ("OCR") announced the launch of the second round of national HIPAA audits. These audits are focused on covered entities (health plans and health care providers) and business associates (e.g., brokers, TPAs). The audits will target enforcement of HIPAA Privacy, Security and Breach Notification rules. OCR plans to conduct desk and onsite audits for both covered entities and their business associates. The first set of audits will be desk audits of covered entities followed by a second round of desk audits of business associates. OCR intends to complete desk audits by the end of December 2016.

Importantly, OCR has indicated that the audit process will begin via email inquiry to a covered entity or business associate, and that some email systems may classify HHS' inquiry as spam:

> 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; OSOCRAudit@hhs.gov.

Click here to view a sample email letter:http://www.hhs.gov/sites/default/files/ocr-address-verification-email.pdf

http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html

Why is OCR Conducting Audits?

As part of the HIPAA HITECH legislation passed in 2009, Congress tasked OCR to begin compliance enforcement of HIPAA's regulatory requirements. OCR began the first phase of the audit program (known as the "audit pilot program") in 2012. The limited number of audits conducted in that round were deemed to be a success, and after securing a $4 million increase in funding from Congress for fiscal year 2016, OCR announced phase two will begin effective March 21, 2016.

Who does this Impact?

HIPAA Privacy and Security applies to insured and self-funded group health plans (includes HRAs and health FSAs).

What does HIPAA Privacy and Security Require?

HIPAA regulations impose significant compliance obligations on covered entities. These include:

- Maintaining plan documents – updated for final rules issued in 2013
- Implementing HIPAA Privacy and Security policies and procedures and administrative safeguards – electronic and physical protection of protected health information ("PHI")
- Establishing procedures to (1) facilitate early detections of potential breaches of unsecured PHI and (2) upon the occurrence of an unauthorized use/disclosure of unsecured PHI have procedures in place to conduct appropriate risk analysis.
- Maintaining Business Associate Agreements ("BAAs") -- the covered entity should have a signed BAA between the plan and any service provider that handles PHI, such as brokers/consultants, TPAs, COBRA vendors, certain payroll vendors, accountants, law firms, etc.
- Distributing the Notice of Privacy Notice (self-funded plans only)
- Conducting regular Security risk assessments
- Complying with tracking and communication requirements of participant requests for PHI
- Conducting training for members of a workforce who handle PHI

Importantly, the OCR audits will cover only federal HIPAA Privacy, Security and Breach Notification rules. No state- or city-specific privacy rules will be included.

What are the Penalties?

According to OCR, the audits are meant to help improve HIPAA compliance, although serious compliance issues could prompt further investigation. HIPAA imposes significant non-compliance penalties on covered entities. Penalties can range from $100 per violation up to $50,000 per violation (in the case of willful neglect), with an annual maximum of $1,500,000 per violation.

What to Do?

Upon notification of an audit, OCR will provide covered entities 10 business days to demonstrate they are following HIPAA Privacy and Security rules.

Covered entities should review their HIPAA policies, procedures, notices and documents now to ensure they are updated for HIPAA HITECH and the final HIPAA omnibus rules. In addition, covered entities should ensure up-to-date business associate agreements have been signed with any service providers with access to PHI.