HIPAA Phase II Audits Are Underway…Will You Be Ready?

Now that the Department of Health & Human Service (HHS), Office of Civil Rights (OCR)[1] has published the long-awaited Phase II Audit Protocols for HIPAA compliance, the process is in full swing.[2] What does this mean to Covered Entities ("CE") and their Business Associates ("BA")? In short, CEs and BAs must make sure that they are in compliance with the Privacy and Security regulations *before* OCR comes calling.

A little Background. The 2009 HITECH Act required HHS to conduct periodic audits to ensure compliance with the HIPAA Privacy, Security and Breach Notification Rules. In 2011, OCR began a pilot audit program to develop a long-term protocol for future audits. Then in 2012 "Phase I" audits applied the initial protocol to audit 115 Covered Entities, both to measure the effectiveness of the protocol and also evaluate the subject CE's efforts with HIPAA compliance and assess the CEs privacy, security and breach notification compliance. Among the more notable findings, OCR determined that 60% of the deficiencies related to the HIPAA Security Rule.[3] Most notably, however, was the finding that two-thirds of the entities audited had not done a complete and accurate risk assessment. While all but a handful of the audited CEs had some level on non-compliance, the most common reason for the deficiency was the CEs lack of understanding or knowledge of the HIPAA requirements. OCR's Phase I findings were a wake-up call to CEs and BAs, alike, insofar as they highlighted risk areas that could lead to significant penalties in the event of a breach. Significantly, the lack of appropriate risk analyses has also been highlighted in settlement and resolution agreements after a breach of PHI was reported to OCR. For example, in late 2015, OCR imposed $750,000 sanctions on two separate CEs for breaches that resulted from security incidents that could have been avoided had an appropriate risk analysis been performed.[4]

DEPARTMENT OF HEALTH AND HUMAN SERVICES OFFICE OF THE SECRETARY

Director
Office for Civil Rights
200 Independence Ave., SW; RM 509F
Washington, DC 20201

DATE

Contact Person's Name
CE/BA Name
Address
City, State ZIP

Dear Contact:

This is an automated communication from the Office for Civil Rights (OCR).

According to our records, you are the primary contact OCR should use to reach Entity Name regarding its potential inclusion in the HIPAA Privacy, Security, and Breach Notification Rules Audit Program. We are attempting to verify this email address.

Please respond within fourteen (14) days as instructed below to either confirm your identity and email address or instead provide updated primary and secondary contact information.

If you ARE the primary contact for this organization, please select the following link YES. Once the link is selected, a browser window will open and your response will be recorded.

If you ARE NOT the primary contact for this organization, please select the following link NO. Once the link is selected, a browser window will open and your response will be recorded.

Thank you for your cooperation. If we do not receive a response from you we will use this email address for future communications with this entity. Failure to respond will not shield your organization from selection.

If you have questions or comments regarding this message, you may contact us at OSOCRAudit@hhs.gov.

Sincerely,

Jocelyn Samuels
Director
Office for Civil Rights
OFFICE OF THE SECRETARY
Department of Health and Human Services
http://www.hhs.gov/ocr

Figure 1

The Phase II OCR Audits.

With the Phase II Audit Protocols now in place, CEs may soon (if they have not already) receive correspondence from OCR seeking background information on its operations. This first step, which many CEs may have already encountered, comes in the form of an email letter from OCR seeking verification of the CEs address and key contact person. [Figure 1].

[1] OCR is the division within HHS tasked with enforcement of the HIPAA/HITECH Law and applicable regulations.
[2] Posted in April 2016, available at: http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html.
[3] Available at: http://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/index.html.
[4] *See* $750,000 HIPAA Settlement Underscores the Need for Organization Wide Risk Analysis -; 750,000 HIPAA Settlement Emphasizes the Importance of Risk Analysis and Device and Media Control Policies.

The second step will be a pre-audit screening questionnaire, also transmitted electronically by OCR, seeking additional information about the potential auditee (CE or BA), including:

- Size
- Number of clinicians
- Affiliations
- Single/multiple locations
- Type of Entity (Provider/Plan/Clearinghouse)
- EMR and other electronically maintained systems (billing, accounting)

OCR will utilize this information to create a pool of potential subjects for its audit. While the preliminary correspondence from OCR indicates that failure to respond will merely cause OCR to use publically available information in its audit pool, the greater risk of ignoring OCR is a potential compliance review (and associated penalties). Because many entities' spam filters may classify OCR's emails as spam or junk, CEs and BAs are cautioned by OCR to periodically check these folders to avoid an untimely response. This is particularly true in the case of an entity being chosen for audit.

OCR will also being asking CE to provide information about all of its BAs for its second round of audits, including 27 specific elements related to each BA. These elements include:

- Business Associate Name
- Type of Service(s) provided
- First Point of Contact Name, Title, Address, phone number(s), fax numbers and email
- Second Point of Contact Name, Title, Address, phone number(s), fax number and email; and
- Website URL

While there is no mandatory format CEs must use to track their BAs, OCR has developed a template the CEs may use to track their BAs. [Figure 2]. Regardless of format, it is imperative for a CE to have this information in place before requested, since response times are incredibly short—many less than 10 days for complete turn-around.

BA Name	Type of Service Provided	POC1 Title	POC1 First Name	POC1 Last Name	POC1 Address	POC1 Address Continued	POC1 City
UNITED COUNSELING SERVICE OF BENNINGTON COUNTY, INC.		HR Director	Amy	Fela	PO BOX 588		BENNINGTON
Asociacion De Maestros De Puerto Rico		President	Aida	Diaz de Rodriguez	452 Ponce de León Ave		San Juan
Idaho Department of Health & Welfare		Privacy Officer	Heidi	Graham	PO Box 83720		Boise
NEXUS LAB, INC.		Interm Compliance Officer	Anna	Whitef	PO Box 1240		RUSSELL SPRINGS
ANTONIO ESPARZA, M.D., P.A.		Office Manager	Irene	Paramo	500 W SAM HOUSTON	SUITE1	PHARR

Figure 2

With the Phase II process underway, it is unclear when OCR will begin the actual audits. What is known is that the Phase II audits will be done in three phases: The first will only involve CEs chosen by random selection from the various pools created through the pre-screening process. The second phase will target BAs. These first two phases will primarily be performed through desk-audits in which the targeted auditee will merely receive an email request from OCR for documentation. Once received, the requested documents are to be electronically submitted to OCR no later than 10 days after receipt of the request. Given this tight turn-around, getting your organization into compliance cannot wait. This is particularly true where the information sought is what is in place ***at the time of the request***. Translation: if you don't already have your policies and

procedures in place, getting them in place when OCR comes calling is not an option. OCR anticipates completion of the desk audits in December 2016.

Once the desk audits are completed, OCR will begin the final series of audits, which will encompass a broader scope of the HIPAA requirements than the desk audits. This final stage will involve on-site audits and may include CEs and BAs that were also subjects of the desk audits.

What's a CE (or BA) to do? "Playing Good Defense" in anticipation of Audits.

With the OCR audits underway, CEs and BAs need to take inventory of their systems and procedures to ensure they are compliant with applicable Federal and State laws and regulations. While not an exhaustive list, for organizations subject to HIPAA, as a starting point for your HIPAA compliance efforts consider the following:

- **HIPAA Policies & Procedures**—If your organization does not currently have appropriate HIPAA policies and procedures, now is the time to develop P&Ps that meet your HIPAA obligations. The HIPAA Rules, specifically the Security Rule, require covered entities to maintain reasonable and appropriate administrative, technical and physical safeguards to protect PHI. OCR recognizes that size of an entity varies, as do available resources, allowing flexibility in the implementation of appropriate safeguards.
- **HIPAA Training**—Under the applicable HIPAA Rules, CEs and BAs must conduct periodic (at least annual) ***training*** of its workforce. If requisite training has not been done and documented, now would be a great time to do so.
- **HIPAA Risk Assessment**—The HIPAA Regulations mandate annual risk assessment to address potential Privacy and Security issues. While there are publicly available tools organizations can utilize to address this requirement and to avoid substantial penalties that can flow from the failure to do so, these analyses can often times be daunting, particularly to smaller providers.
- **Updates to Business Associate Agreements and business operations to comply with the Telephone Consumer Protection Act (TCPA):** CEs subject to HIPAA's marketing limitations must adhere to both the TCPA mandates and HIPAA regulations. Given recent Declaratory Rulings from the FCC, Business Associate Agreements must be updated to clarify the procedures to follow for non-marketing informational calls relating to health care and to address TCPA mandates relating to marketing activities performed on behalf of a covered entity.
- **General Compliance & FWA Training** –Although not a Privacy issue, general compliance efforts should not be ignored. Anyone participating in Medicare Part C & D (MCOs and Prescription Drug Plan Sponsors and their first-tier, downstream and related entities (FDRs)) are required to conduct general compliance and fraud, waste and abuse (FWA) training at least annually (and within 90 days of hire). Any entity that qualifies for such training must ensure that appropriate training is conducted and documented.

HIPAA audits are now a reality and the incidence of receiving an audit request is on the rise. Waiting for the proverbial axe to fall is unwise, particularly in light of the significant costs and fines associated with a data breach. According to a 2015 survey conducted by the Ponemon Institute,[5] the average cost for a data breach

[5] Available at: http://www-03.ibm.com/security/data-breach/

in 2014 was around $3.8M. Add in the damage to an organization's reputation, and the effects can be devastating.

Assessing *what* is required and implementing a timeframe for doing so now will ensure that any issues identified along the way can and will be remedied timely and efficiently. The list above is by no means exhaustive, but is intended to jump-start your efforts in this New Year.

In the immortal words of Benjamin Franklin—*An ounce of prevention is worth a pound of cure*.

The AccuMed Group welcomes the opportunity to help you evaluate if your department and community are benefiting from the level of results and accountability you deserve. AccuMed can assist in your HIPAA and general compliance activities on the billing side, including conducting a cost free analysis of your current billing, compliance and reporting effectiveness. Once the analysis is complete you will be in a position to create a compliance plan which will be OIG and HHS friendly. AccuMed can also assist with getting you in touch with other high level resources if further insight or assistance is needed. For further information, please visit our website at www.theaccumedgroup.com or contact any member of The AccuMed Team.

Dawn O'Connell
800.926.6985 x 222
dawn@theaccumedgroup.com

Kate Melasi
810.750.1145
kate@theaccumedgroup.com