Office of Civil Rights on HIPAA Phase 2 Audits: “We are not playing a ‘gotcha’ game”

On July 11, the Department of Health and Human Services Office for Civil Rights (OCR) kicked off its HIPAA Phase 2 audits with correspondence to 167 covered entities. Responses to the initial questions were required by July 22, but, as the letter stated, “Failure to respond will not shield your organization from selection.” However, it’s too soon for those entities not in receipt of a letter or email to celebrate—they are still eligible to be chosen for an onsite audit in the early part of 2017.

Covered entities selected at random

The entities audited in this stage of Phase 2 include hospitals, nursing homes, health systems, pharmacies, medical practices, skilled nursing facilities and elder care nursing facilities. A computerized process selected the covered entities at random from a list of more than 10,000 covered entities that had filled out “pre-audit questionnaires.” The selection process was designed to result in a balanced geographic distribution.

OCR’s Phase 2 audit program was announced in March, and the Office released Phase 2 protocols the following month. Considering the breadth of the procedures outlined, many predicted that the desk audits would involve a large swath of HIPAA criteria. It turns out that that’s not the case.

It’s all about HIPAA Privacy, Security, and Breach Notification…

Rather than evaluate HIPAA compliance through a wide lens, this round of audits will concentrate on the HIPAA Privacy, Security and Breach Notification Rules. More specifically, the OCR will assess the entity’s notice of privacy practices (including provision notice, electronic notice, and whether content requirements are being met; also, patient right of access to protected health information [PHI]). Under the Security Rule, the entity’s risk analysis and risk management will be evaluated. And finally, the Breach of Notification Rule: In the event of a breach, what is the content of the notification? And how timely is the notice?

The audit process itself relies heavily on the entity’s documentation of its own compliance. The entity is expected to use an OCR portal (recently created for this purpose) to upload the necessary verification. Therefore, there is no room for an entity to include exposition or commentary or to attempt to justify potential non-compliance.

OCR fields questions from auditees and Director offers reassurance

Two days after the initial notices were sent informing the entities of the audit, the OCR held a webinar with the goal of addressing auditee questions. During that event, OCR Director Jocelyn Samuels stressed that the OCR was

seeking to gather data regarding HIPAA compliance in the industry with the goal of creating new guidance documents and instruments for compliance. “We are not playing a ‘gotcha’ game,” she said, “this is not intended to be a punitive process.”

However, Samuels added that if OCR discovers “significant threats” to the security and privacy of PHI, OCR may choose to exercise enforcement. Otherwise, if OCR determines that good faith efforts were made to be compliant with HIPAA regulations, this round of audits will not culminate in punishment.

Looking ahead, the second round of Phase 2 audits is set to begin in September, and will involve over 30 business associates (the first inclusion of business associates in these HIPAA audits).

The third round of Phase 2 audits is set to begin in early 2017 and will entail onsite audits of covered entities and business associates, also chosen through the random computerized process that selected the current auditees. The entities involved in this first round of audits will not be included in the onsite audits.

For more information/questions regarding any legal matters, please email info@nelsonhardiman.com or call 310.203.2800.