

HHS Office for Civil Rights in Action



OCR Cyber-Awareness Monthly Update March 21, 2016

OCR Launches Phase 2 of HIPAA Audit Program

As a part of its continued efforts to assess compliance with the HIPAA Privacy, Security and Breach Notification Rules, the HHS Office for Civil Rights (OCR) has begun its next phase of audits of covered entities and their business associates.

Audits are an important compliance tool for OCR that supplements OCR's other enforcement tools, such as complaint investigations and compliance reviews. These tools enable OCR to identify best practices and proactively uncover and address risks and vulnerabilities to protected health information (PHI).

In its **2016 Phase 2 HIPAA Audit Program**, OCR will review the policies and procedures adopted and employed by covered entities and their business associates to meet selected standards and implementation specifications of the Privacy, Security, and Breach Notification Rules. These audits will primarily be desk audits, although some on-site audits will be conducted.

The 2016 audit process begins with verification of an entity's address and contact information. An email is being sent to covered entities and business associates requesting that contact information be provided to OCR in a timely manner. OCR will then transmit a pre-audit questionnaire to gather data about the size, type, and operations of potential audit subjects; this data will be used with other information to create potential audit subject pools.

If an entity does not respond to OCR's request to verify its contact information or pre-audit questionnaire, OCR will use publically available information about the entity to create its audit subject pool. Therefore an entity that does not respond to OCR may still be selected for an audit or subject to a compliance review.

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 entities to check their junk or spam email folder for emails from OCR.

The audit program is developing on pace and OCR is committed to transparency about the process.

OCR will post updated audit protocols on its website closer to conducting the 2016 audits. The audit protocol will be updated to reflect the HIPAA Omnibus Rulemaking and can be used as a tool by organizations to conduct their own internal self-audits as part of their HIPAA compliance activities.

OCR's audits will enhance industry awareness of compliance obligations and enable OCR to better target technical assistance regarding problems identified through the audits. Through the information gleaned from the audits, OCR will develop tools and guidance to assist the industry in compliance self-evaluation and in preventing breaches. We will evaluate the results and procedures used in our phase 2 audits to develop our permanent audit program.

Additional details and useful information about OCR's Phase 2 Audit program area easily accessible on this website: <http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html>.

