What to Expect from the OCR Audits

By Bridgette O'Connor
PHI365 Manager, GRA Benefits Group

The federal government is serious about HIPAA compliance. The next round of compliance audits encompasses more than three times as many companies as the pilot audits. Reputational and financial consequences are expected for any companies failing to protect health information.

The Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) is resuming its HIPAA compliance audit program this fall. The focus will be on "desk audits," with comprehensive on-site audits as resources allow. OCR has notified and plans to audit 350 covered entities and 50 business associates. Covered entities are carriers, hospitals and doctor offices. Business associates are vendors of covered entities: insurance agents, IT vendors and medical transcriptionists.

The focus of business associate audits will be on HIPAA security risk analysis and risk management, as well as breach reporting to covered entities. Looking ahead to 2015 and 2016, OCR expects audits to focus on physical access and technical security – computing device and storage media security controls, transmission security, encryption.

During the pilot round of audits in 2012, OCR determined a major weakness was the lack of a risk analysis. If you are found without a documented risk analysis, OCR will issue harsh penalties. HHS released a risk assessment tool for covered entities and business associates to use. It can be found here: http://www.healthit.gov/providers-professionals/security-risk-assessment. This should be the first step any HIPAA compliant organization takes.

If you aren't in those first business associates, it doesn't mean you won't be affected this fall. You could be under a covered entity who is audited, who may in turn audit your agency.

OCR is setting themselves up for a permanent audit program, by funding future audits with fines imposed through investigations and audits. Ensuring a continuation of yearly audits and increasing agents' chances of coming in front of OCR.

Audits are just one source of HIPAA compliance penalties. A bigger concern for insurance agents should be breaches. If you have a breach, you will be subjected to an OCR investigation. Then there's always patient and client complaints that continue to be a source for thousands of investigations.

Fortunately, OCR has made the audits a little easier by identifying their focus areas. Even if you aren't being audited by OCR, your carrier could audit you or you could experience an audit in coming years. It is vital for your agency to take a look at the audit focus areas, make sure your policies are up to date and perform a mock audit on your agency.

The current audit protocol is available at: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html. The updated audit protocol is expected to be available for organizations' own internal compliance assessments, possibly this year.

It is vital for your agency to take a look at the audit focus areas, make sure your policies are up to date and perform a mock audit on your agency.

Key Compliance Tasks

- *Risk Analysis.* Confirm you have an up-to-date risk analysis and a corresponding risk management plan to show you are bringing risks down to reasonable and appropriate levels. If you haven't done a risk analysis, look into a third-party vendor to perform one. Federal auditors look favorably on companies using an outside

vendor, as they consider vendors unbiased. Performing a risk analysis will determine threats and vulnerabilities to your organization's protected health information. The results then guide you in developing the appropriate policies and procedures.

- *Documentation.* With 'desk audits,' the emphasis will be on up-to-date documentation. Begin compiling that documentation now or ensure it is updated for 2014. Most documentation should be reviewed at least annually. Examples of required documentation include a risk analysis, disaster recovery plan, employee handbook, breach notification policy and information technology procedures.
- *Breach Notification.* Confirm your breach notification procedures are in line with the 2013 Omnibus Rule update. The new guidelines offer four factors for identifying whether an impermissible use or disclosure was a breach. Also, determine a way to document your assessment of the breach and the results; options include a checklist or spreadsheet.
- *Technical Security.* The goal is to protect information while adopting new technologies. Your technical security controls should be based off your risk analysis. Controls include email encryption, user access, mobile device security, strong passwords, system testing and malware protection. Technical security is a significant trend in the compliance community. A majority of 2014 breaches were due to unsecured mobile devices. Microsoft Windows users should also note that using Windows XP without implementing further protections, may greatly increase risk to your client information and potential fines.
- *Training.* All employees should be trained on the proper handling of sensitive information. Some agencies create their own program, others utilize an online training provider. Training shouldn't be a one-and-done process. HIPAA is always changing and new guidance is released every few months, therefore periodic reminders and annual training are essential. ■

As the PHI365 manager at GRA Benefits Group, Bridgette O'Connor consults with agents on moving toward HIPAA and Gramm-Leach-Bliley compliance.