HIPAA Audits for 2012

Are You Prepared?

The U.S. Department of Health and Human Services Office for Civil Rights (OCR) announced a pilot program for auditing covered entities under HIPAA. These audits are a requirement of the 2009 HITECH Act. The audits began in late 2011 and will continue through 2012 until 150 audits have been conducted. The OCR will use these audits to assess compliance in privacy and security and to design future audits. The goal of the pilot program is to identify areas of health information breaches, as well as best practices, in order to help the OCR develop technical assistance to covered entities.

The OCR web site states that "Every covered entity and business associate is eligible for an audit." This includes health care providers and employer-sponsored group health plans. Since this is a pilot program, the OCR plans on selecting a broad range of health care entities to include all types and sizes. Until now, audits had been performed on covered entities that had a complaint filed against them. The new rule calls for audits regardless of whether a complaint has been filed.

If selected for an audit, covered entities should be prepared to respond to requests for documentation during the audit period. For example, the privacy standards require that covered entities document certain elements of their privacy compliance plans, including:

- Policies and procedures
- Privacy notices
- Business associate agreements/contracts
- Staff training
- Complaints
- Disposition of complaints
- Any sanctions levied against staff members

Covered entities need to maintain a list of these elements, including their location within the practice. Following a request for documentation, you will have 10 days to provide these materials.

The audit will include a site visit to interview key personnel, as well as observe processes and operations to determine if HIPAA privacy and security measures are being met. Depending on the size of the organization, the OCR anticipates that the on-site visit will take between three to 10 business days. The auditors will provide a detailed report to the covered entity following the audit. The covered entities will have an opportunity to review the report with the OCR and implement corrective actions on deficiencies.

(continued on next page)

PROFESSIONALS ADVOCATE®
Insurance Company

How should you prepare in the event that your practice is selected for one of the pilot audits? A starting point for any practice is to conduct your own self-audit. Reviewing and updating your privacy and security plans is an important first step in the self-audit process. If you have not updated your policies since their inception, now is the time to do so to ensure their accuracy. Have there been any name changes or changes in process in releasing protected health information (PHI) under your HIPAA privacy policy? Does all of your staff follow the privacy and security policies put in place? Have you performed a self-test on the security of your electronic communication under your HIPAA security policy? Are you or your health care providers sending email with protected health information using unprotected web addresses? Popular web-based email sites, such as Gmail, Yahoo! Mail and Hotmail, are not encrypted and are not protected by a patient portal. Therefore, sites like these should not be used to communicate PHI.

Bottom-line, practices will need to place a high priority on HIPAA privacy and security compliance.

Complete information regarding the new audit program, including anticipated timelines and on-site visits, may be found at: *http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html.*

Additionally, the Maryland Health Care Commission has several useful web tools to help you determine your readiness for a HIPAA audit on their web site: *http://mhcc.maryland.gov/edi/practicemanagement.html.*

Sample Questions to Ask Yourself:

- Do you have written HIPAA privacy and security policies and procedures in place?
- Is your notice of privacy practices up to date?
- Do you have annual staff training on HIPAA?
- How do you educate new hires on HIPAA?
- Do you have your staff sign confidentiality agreements?
- Do you have signed business associate agreements on file?
- Do you allow PHI to be removed from the practice?
- What steps have you taken to encrypt PHI?
- Does the practice have a designated privacy officer?
- Are staff work stations secure?
- Do you have a disciplinary policy for staff members who violate privacy or security?
- Do you know what to do when there's a breach?
- How do you dispose of PHI?

PROFESSIONALS ADVOCATE®
Insurance Company

ProAd offers additional risk management resources to you on our web site: **proad.com**

Virginia Office
804 Moorefield Park Drive
Richmond, VA 23236
804-320-6790
888-411-0444 (toll free)
866-579-1948 (toll free)

Home Office
225 International Circle
Hunt Valley, MD 21030
410-785-0050
800-492-0193 (toll free)