



June 11, 2012

Five steps to protect your organization from HIPAA audits

By Neda Mirafzali, JD

Violations of the [Health Information Portability and Accountability Act of 1996](#) (HIPAA), are serious business for behavioral health professionals. It is not uncommon for such violations to cost healthcare providers more than \$1 million in penalties or settlements.

Until recently, such settlements and penalties arose almost exclusively from patient complaints alleging compromised protected health information. Now, psychiatrists, psychologists, therapists and other behavioral health practitioners must be wary of a new source – the HIPAA audit.

The audits are made possible under Section 13411 of the American Recovery and Reinvestment Act of 2009, which established the Health Information Technology for Economic and Clinical Health (HITECH) Act. The Department of Health and Human Services (HHS) Office of Civil Rights (OCR) has engaged KPMG, LLC to conduct pilot audits of covered entities to run through December 2012.

The pilot will include audits of up to 150 covered entities of all sizes. This can include any healthcare provider that transmits health information in electronic form. Behavioral healthcare providers, psychologists, psychiatric clinics, behavioral health managed care companies, psychiatric hospitals and others all are at risk.

Audit process

An audit begins with a notification letter requesting evidence of a covered entity's HIPAA privacy and security compliance efforts. Thirty to 90 days following receipt of the requested information, KPMG will conduct an on-site visit. The on-site visit will include interviews with the entity's leadership, examination of the physical space and operations, review of consistency of the entity's practice with its stated policies and observation of the entity's compliance with the HIPAA rules.

Based on its findings, KPMG drafts a report and turns it over to the audited entity for review. Within 10 business days, covered entities may provide written comments, concerns and corrective actions taken to address any potential violations. KPMG then provides a final report to OCR.

Steps to prepare and protect

This year's pilot period provides behavioral health entities with an opportunity to prepare themselves for an audit. Below are five steps to HIPAA audit protection.

- **Update or create HIPAA policies.** A policy drafted even a few years ago may be out-of-date. Where policies have not been updated recently, work with a professional specializing in HIPAA compliance to have them reviewed and brought up-to-date.
- **Train or retrain staff.** This is a prime time for behavioral health staff to be trained or re-trained on HIPAA and an organization's own policies, the necessary requirements for compliance and the consequences for noncompliance. Seek expert assistance in establishing training procedures.
- **Enforce policies.** During the audits, OCR will be looking at whether HIPAA policies are enforced. Failure to enforce policies may put the entity in a worse position than not having a policy at all.
- **Explore new risks and vulnerabilities.** Behavioral health entities should familiarize themselves with new risks and vulnerabilities for breaches of patient information. Two emerging concerns are the appearance of patient information on social media sites and the use of portable storage devices, like flash drives and laptops, to transport unencrypted data. Most breaches of patient information are unintentional, so professionals should guard against these risks by educating staff on proper and improper use of such tools.
- **Look out for new rules.** Behavioral health entities can expect HHS to issue new rules on breach notification this year, finalizing its Interim Final Rule issued in August 2009. Behavioral health entities should pay attention to new rules and ensure they are incorporated into HIPAA compliance policies.

Most behavioral health entities will not be audited this year, but everyone needs to be prepared. All behavioral health entities should take this opportunity to dust off their HIPAA compliance policies and ensure they reflect the most updated regulations. This benefits both the organization's patients and its business.

Neda Mirafzali, Esq. is an associate with Clark Hill, PLC in the firm's Birmingham, Mich. office. Ms. Mirafzali practices in all areas of healthcare law, assisting clients with transactional and corporate matters; providing counsel regarding compliance and reimbursement matters; representing providers and suppliers in behavioral healthcare litigation matters in third party payor audit appeals. She can be reached at nmirafzali@clarkhill.com.

Source URL: <http://www.behavioral.net/article/five-steps-protect-your-organization-hipaa-audits>