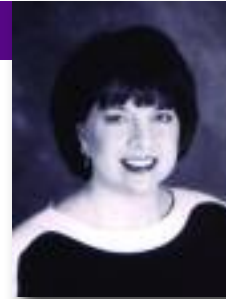


# HIPAA Enforcement and the Physician Practice



By Ann Bachman, MT (ASCP), CLC (AMT)

Private practices are now being investigated for HIPAA violations! In fact, the Office of Civil Rights has received more HIPAA-related complaints against private practices than any other segment of the healthcare industry.

Since April 14, 2003, Health and Human Services Office of Civil Rights (OCR) has received over 27,070 HIPAA Privacy complaints. It has investigated and resolved over 4,577 cases, applying corrective measures in all cases where an investigation indicates noncompliance by the covered entity, including: national pharmacy chains; major medical centers; health plans, hospital chains; and small provider offices.

In the rest of completed cases (16,500), the investigations found no violation had occurred or the complaint did not present an eligible case for enforcement, including: alleged violations before the compliance date or complaints against an entity not covered by the Privacy Rule; the complaint was untimely or was withdrawn or not pursued by the complainant; or the activity described does not violate the Rule, such as when the covered entity has disclosed protected health information in permitted circumstances. The compliance issues investigated most often are, in order of frequency:

- Impermissible uses and disclosures of protected health information;
- Lack of safeguards of protected health information;
- Lack of patient access to their protected health information;
- Uses or disclosures of more than the Minimum Necessary protected health information; and
- Lack of or invalid authorizations for uses and disclosures of protected health information.

The most common types of covered entities required to take corrective action to achieve voluntary compliance are, in order of frequency: private practices; general hospi-

tals; outpatient facilities; health plans (group health plans and health insurance issuers); and pharmacies.

Cases involving the knowing disclosure or obtaining of protected health information in violation of the Rule are referred to the Department of Justice (DOJ) for criminal investigation. To date, OCR has made over 393 such referrals to DOJ.

## SECURITY VIOLATIONS

Cases that may be violations of the HIPAA Security Rule are referred to the Centers for Medicare and Medicaid Services (CMS); since April 30, 2007, the OCR has made over 153 such referrals. In referred cases that describe potential violations of both the HIPAA Privacy and Security Rules, OCR and CMS coordinate investigations.

## PRIVACY COMPLAINT INVESTIGATION

The OCR does not investigate every complaint received. To trigger an investigation or inspection, complaints must meet certain criteria:

- The alleged violation must have occurred after April 12, 2003.
- The complaint must be filed against a covered entity. Not every business or agency is subject to the HIPAA regulations. For example, employers are not held to the HIPAA regulations unless they are also "covered entities."
- The complaint must be about an activity that, if proven true, would be a violation of the Privacy Rule.
- The OCR must know the identity of the person who initiated the complaint and must have a way to contact that individual.
- The OCR may have to release the name of the person who initiated the complaint during the investigation.

## INVESTIGATIONS AND YOUR PRACTICE

What does this enforcement activity mean for your practice? It means now is the

time to get serious about compliance if you have not already done so. Effective HIPAA compliance includes a comprehensive, written plan, periodic audits, and extensive employee training. The written plan must include disciplinary actions, and any disciplinary actions taken must be documented.

If you have a written plan but it is on a shelf collecting dust, get it out and get busy. Conduct a HIPAA audit of your practice, perhaps enlisting the assistance of a "secret shopper." If your staff knows you are auditing for HIPAA violations, they will be on their best behavior!

Following the audit, schedule an employee training session to discuss the findings as well as reminders about the importance of maintaining security and privacy of all patient information. Give them an opportunity to ask questions and air their concerns. Make sure every employee understands your procedure for reporting potential violations and that there will be no retaliation for reporting problems.

Remember, HIPAA compliance must cover your entire workforce, which includes employers, volunteers and students, and audits and training are to be repeated periodically.

Document, document, document! If you become the subject of a HIPAA investigation, this may help prevent monetary penalties. ■

*Ms. Bachman is director of the Compliance Department at DoctorsManagement. For additional assistance with your HIPAA program, contact DoctorsManagement at 800-635-4040.*

**DoctorsManagement, LLC, is a TMA Corporate Partner.** This information was supplied by DoctorsManagement exclusively and for the benefit of our members. TMA does not accept responsibility for the information provided.