hfm
healthcare financial management association www.hfma.org

Linda S. Ross
Michael J. Friedman

HIPAA privacy audit tool

Many covered entities (healthcare providers, health plans, and healthcare clearinghouses) heaved a sigh of relief after finalizing their Health Insurance Portability and Accountability Act Notice of Privacy Practices, adopting policies and procedures, and conducting workforce training. Reports from the U.S. Department of Health and Human Services Office of Civil Rights, which is charged with enforcing the privacy rule, however, indicate that complacency comes at a price. As of Nov. 8, 2005, 16,175 complaints have been filed with OCR, and conversations with OCR representatives indicate that complaints are being filed at an increasing rate.

Approximately one-half of all complaints received have focused on impermissible disclosures or disclosures that the complainant thought were improper. From the covered entity's perspective, the greatest problem has been rogue employees—those who do not follow the privacy policies and procedures. OCR notes that, so far, only a small number of complaints have led to civil penalties. As time goes by and the necessary compliance steps are presumed to be better understood and implemented, however, OCR expects the number of complaints that result in civil penalties will increase. In other words, OCR will be less tolerant of well-intentioned mistakes, omissions, and failures.

HIPAA violations typically arise when real-life situations demonstrate shortcomings in a covered entity's notice of privacy practices, policies and procedures, or the extent to which the covered entity's workforce complies (or fails to comply) with those NPPs, policies, and procedures. Adoption of NPPs and policies and procedures and completion of initial workforce training are preliminary, but by no means the final, steps in ensuring HIPAA compliance.

In light of increased levels of complaint investigations and referrals to the U.S. Department of Justice, covered entities would be wise to audit their HIPAA compliance as part of their commitment to compliance and risk management.

A HIPAA self-audit should include two phases. The first phase is to examine the extent to which the covered entity has met the documentation requirements mandated by the HIPAA statute and regulations. The second, and perhaps more important, phase is to assess the extent to which the covered entity and its workforce are actually complying with the HIPAA compliance policies, procedures, forms, and initiatives instituted by the covered entity. This phase should involve on-site visits to various locations of the covered entity where personal health information is used or disclosed and should include observations of daily operations involving the use and disclosure of PHI, such as in a waiting room of a particular hospital clinic. It also should include monitoring access to PHI and steps taken when improper access is discovered.

The number of blatant yet correctible HIPAA violations that occur regularly is surprising. Identifying your own HIPAA shortcomings enables you to correct them and reduce the risk of HIPAA violations and the commitment of personnel, time, and financial resources required to respond to a government-initiated investigation. ●

SELF-AUDIT TOOL

The form that follows is one of nearly 100 templates that comprise an integrated toolkit developed to help covered entities assess their HIPAA compliance. This assessment consists of a review of documentation/policies and an on-site review of compliance practices. The template focuses on business associates and is intended for use during an on-site review of compliance practices.

Linda S. Ross is a partner, Health Care Department, Honigman Miller Schwartz and Cohn LLP, Detroit (lross@honigman.com).

Michael J. Friedman is a partner, Employee Benefits Department, Honigman Miller Schwartz and Cohn LLP, Detroit (mfriedman@honigman.com).

HIPAA PRIVACY AUDIT TOOL
ON-SITE REVIEW
BUSINESS ASSOCIATE COMPLIANCE

_____

[Insert Covered Entity Name]

_____

[Insert Dates of Review]

_____

[Reviewer's Initials]

OPERATIONAL CONSIDERATIONS	OBSERVATIONS	RECOMMENDATIONS
A. Is there an organized, consistent method for identifying business associates and determining when a business associate agreement is required? Describe. ☐ Yes ☐ No ☐ Partial ☐ N/A ☐ See Comments		
B. Are business associate agreements complete, signed, centralized, and monitored? How and where? ☐ Yes ☐ No ☐ Partial ☐ N/A ☐ See Comments		
C. Is someone responsible for administering and monitoring the business associate agreement process? ☐ Yes ☐ No ☐ Partial ☐ N/A ☐ See Comments		
D. Is someone responsible for negotiating changes to business associate agreements? ☐ Yes ☐ No ☐ Partial ☐ N/A ☐ See Comments		
E. Does the Covered Entity have a system in place to address any patterns of activity or practice of business associates that constitute a material breach or violation of the business associates' obligations? ☐ Yes ☐ No ☐ Partial ☐ N/A ☐ See Comments		

OPERATIONAL CONSIDERATIONS	OBSERVATIONS	RECOMMENDATIONS
F. Is the Covered Entity aware of any patterns of activity or practice of business associates that constitute a material breach or violation of the business associate's obligations? ☐ Yes ☐ No ☐ Partial ☐ N/A ☐ See Comments		
G. If so, has the Covered Entity taken reasonable steps to cure the breach, or, if unsuccessful, either terminate the contract or report the problem to the Secretary? ☐ Yes ☐ No ☐ Partial ☐ N/A ☐ See Comments		
H. Does the Covered Entity have business associate contracts in place with such entities as its accreditation organizations and its professional advisers (e.g., attorneys, CPAs, consultants)? ☐ Yes ☐ No ☐ Partial ☐ N/A ☐ See Comments		
I. Is this Covered Entity or any of its business associates a governmental entity? If so, specify. ☐ Yes ☐ No ☐ Partial ☐ N/A ☐ See Comments		
J. Do any circumstances exist whereby PHI is disclosed to a business associate in accordance with legal requirements without obtaining a business associate contract when a business associate contract would otherwise be required? Describe. ☐ Yes ☐ No ☐ Partial ☐ N/A ☐ See Comments		
K. If so, are satisfactory assurances obtained to protect the information or is failure to obtain satisfactory assurances documented? ☐ Yes ☐ No ☐ Partial ☐ N/A ☐ See Comments		

OPERATIONAL CONSIDERATIONS	OBSERVATIONS	RECOMMENDATIONS
L. Is the Covered Entity a business associate of any other covered entities? ☐ Yes ☐ No ☐ Partial ☐ N/A ☐ See Comments		
1) If so, is there a mechanism by which its business associate duties are implemented and monitored? ☐ Yes ☐ No ☐ Partial ☐ N/A ☐ See Comments		
M. Does the Covered Entity utilize its own form of business associate agreement? ☐ Yes ☐ No ☐ Partial ☐ N/A ☐ See Comments		
N. If the Covered Entity accepts other forms of business associate agreements, are they reviewed for compliance with the privacy rule? ☐ Yes ☐ No ☐ Partial ☐ N/A ☐ See Comments		
O. Is staff familiar and compliant with this aspect of the HIPAA rule? ☐ Yes ☐ No ☐ Partial ☐ N/A ☐ See Comments		
P. Are there any other relevant observations? ☐ Yes ☐ No ☐ Partial ☐ N/A ☐ See Comments		

II. Persons Interviewed by Name, Location, and Date

Name/Title: **Location:** **Date:**

1. _____

2. _____

3. _____

Reprinted from the February 2006 issue of *Healthcare Financial Management.*