HHS Commences the HIPAA Audit Program

By Sara Shanti, Fatema Zanzi and George Kendall

The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) has begun auditing covered entities for compliance with the Health Insurance Portability and Accountability Act (HIPAA) under the HIPAA Audit Program (Audit Program). The Audit Program is funded by the Health Information Technology for Economic Clinical Health (HITECH) Act and requires HHS to conduct periodic audits to ensure both covered entities and business associates are complying with the HIPAA Privacy and Security Rules, as well as all Breach Notification standards.

This first round of audits is being conducted through OCR’s Pilot Phase. OCR, the agency which enforces the HIPAA Privacy and Security Rules, anticipates that it will audit approximately 150 covered entities through December 2012. Under the Audit Program, every covered entity and business associate is eligible for an audit. However, based on the objectives of the Pilot Phase, OCR will only audit a range of covered entities, including small provider practices, medical centers, insurance companies, local pharmacies, and national health care chains. While covered entities of all sizes and functions are subject to an audit in 2012, OCR intends to include business associates in future audits.

Last week, OCR stated that the first 20 audits have been conducted, and the remaining covered entities slated for audits in 2012 will be notified within the next few weeks. OCR also stated that the audits have already uncovered significant security vulnerabilities.

OCR Enforcement

Historically, OCR’s enforcement has been complaint driven; however, the agency has become increasingly proactive in sighting out noncompliance and opening compliance reviews. The Audit Program is a formal method of this proactive approach, as it allows OCR to examine the methods, policies and procedures, compliance risks, and vulnerabilities of a selected entity by initiating an audit.

Although OCR states that the Audit Program is not an official investigation, where an audit uncovers compliance concerns, covered entities and business associates will be subject to an official compliance review. Compliance reviews can result in civil monetary penalties (CMPs) of up to $50,000 per violation, and corrective action plans (CAPs), which have the potential to remain in effect for years after an entity has achieved full compliance.
Audit Process

All audits conducted under the Pilot Phase will consist of a document review, including all applicable privacy and security policies and procedures, as well as an onsite visit from OCR. OCR will conduct these audits through government contractor KPMG LLP, using accepted Government Auditing Standards issued by the Government Accountability Office. KPMG's requests during the audit will carry the full weight of the federal government.

If selected to participate in the Audit Program, an entity will receive written notification of the audit. The entity will then have 10 days to provide the requested documentation and a minimum of 30 days to prepare for the onsite visit. The site visit will extend anywhere from three to 10 days and likely include the interviewing of key staff members and the observance of physical plant operations.

Upon reviewing the entity’s Data Response, observing the physical plant, and documenting its findings, KPMG will draft a report to OCR for review and, if appropriate, possible enforcement action. Each audit will result in a report issuing a statement of compliance findings. The selected entity will be provided with a copy of the draft report prior to final submission to OCR, and the entity will have 10 days to provide a written response to this report’s findings. Before finalization, the auditors will include in the report any steps the entity has taken to resolve identified compliance concerns.

In the Pilot Phase, and through the entire Audit Program, OCR is specifically looking for entities to have in place a full set of compliant policies and procedures. Failing to have a complete set of policies and procedures that are reasonably designed for the entity allows the auditors to immediately uncover noncompliance. Failing to have physical safeguards in place is another easily observed area of noncompliance. Considering the HIPAA Privacy Rule has been in effect for nearly 10 years, OCR is likely to have little tolerance for these kinds of violations.

OCR’s Post-Audit Action

Notwithstanding the discovery of a HIPAA violation resulting in a compliance review or other enforcement, OCR will not publically post the findings or participation of individual entities. At this time, OCR plans to use the audit reports to better understand the compliance challenges covered entities face and what technical and other guidance may be most valuable in the agency’s efforts to provide ongoing assistance.

OCR will continue to accept complaints from consumers and members of the industry, but it hopes the Audit Program’s proactive approach will generate greater insight into the status of HIPAA compliance efforts and practices. OCR has stated that it will also share the results of the Pilot Phase so as to promote best practices and address specific compliance issues.

1 See http://www.gao.gov/yellowbook.
Audit Preparation

Although covered entities and business associates do not need to be concerned about unscheduled or undercover auditing, there are several steps entities can take to prepare for an audit. Such steps will also help support an entity’s HIPAA compliance, should an investigation be launched pursuant to an independent complaint.

In general, covered entities and business associates must be prepared to respond to an OCR Data Request. OCR directly contacts Privacy Officers, Legal Departments or Chief Executive Officers when attempting to communicate with an entity. Establishing a good point of contact is important early on in an OCR audit or investigation. Knowledge of whether the requested information exists and where such information is located is also important in providing a complete and timely response.

**Steps Covered Entities and Business Associates Can Take to be Prepared for a Possible Audit**

> Centralize HIPAA compliance documents, including:
>  - Privacy and Security Rule notices, policies, and procedures,
>  - Medical record request forms,
>  - Staff training dates and educational training material,
>  - Security Rule risk analyses,
>  - Breach Notification protocols,
>  - Business Associate Agreements, and
>  - Any documentation regarding mitigating or corrective action measures in conjunction with incidents of noncompliance.

> Review Privacy and Security Rule policies and procedures for adequacy;
> Identify policies and procedures not currently or properly implemented;
> Ensure safeguard protocols are properly implemented and system vulnerabilities are documented and actively addressed; and
> Identify key staff to whom auditors should speak, including:
>  - Chief Information Officer,
>  - Medical Records Director, and
>  - Compliance Officers.

> Confirm key staff is well-versed in the privacy and security policies, staff training initiatives, and internal grievance processes;
> Confirm staff is trained and aware of the personal liability associated with HIPAA noncompliance; and
> Prepare to fully cooperate and accommodate OCR and its auditors.
OCR has previously addressed the unresponsive and uncooperative behavior of an entity with severe enforcement action. On the other hand, OCR has welcomed the opportunity to provide technical assistance to entities and, in the past, has favorably considered an entity’s voluntary corrective actions.

**Future Enforcement**

President Obama has proposed a five-to-eight percent cut for OCR’s 2013 fiscal year budget. Nevertheless, OCR has no intention of curbing the Audit Program or its enforcement actions. In fact, OCR staff has stated that it is looking to take greater control over its enforcement ability by focusing on increased efficiency and high-impact cases.

As provided for under the HITECH Act, CMPs issued by OCR for noncompliance are also retained by the agency. Because of this arrangement, there is concern OCR budget cuts will create an incentive for OCR to pursue enforcement actions resulting in CMPs. Although OCR states that it is committed to transparency, since 2010, it has been significantly more aggressive in pursuing enforcement and compliance through CMPs. Moreover, the HITECH Act has increased the minimum penalty amount for HIPAA violations in addition to issuing a “willful neglect” standard. Where “willful neglect” exists, CMPs must be imposed. Therefore, it is expected penalties for noncompliance will be issued with more frequency and in much greater amounts.

**Sara H. Shanti** is an associate in the firm’s Health Care Practice Group and a former federal investigator for the Office for Civil Rights of the United States Department of Health and Human Services. While at OCR, Sara conducted investigations of alleged violations of federal regulations, and enforced and provided guidance on federal civil rights laws, HIPAA and the HITECH Act. Currently, she focuses her practice on representation of health care providers and clinical researchers in privacy compliance and health care regulatory matters.
Health Care Practice Group

Matthew P. Amodeo  
(518) 862-7468  
Matthew.Amodeo@dbr.com

Christopher B. Anderson  
(312) 569-1257  
Christopher.Anderson@dbr.com

Keith R. Anderson  
(312) 569-1278  
Keith.Anderson@dbr.com

James A. Barker  
(202) 230-5166  
James.Barker@dbr.com

Elizabeth D. Battreall  
(202) 230-5156  
Elizabeth.battreall@dbr.com

Eric M. Berman  
(414) 221-6080  
Eric.Berman@dbr.com

Jennifer R. Breuer  
(312) 569-1256  
Jennifer.Breuer@dbr.com

Brett Bush  
(518) 452-8787  
Brett.Bush@dbr.com

Eileen M. Considine  
(518) 862-7462  
Eileen.Considine@dbr.com

Stanley W. Crosley  
(317) 770-7399  
Stanley.Crosley@dbr.com

John J. D’Andrea  
(518) 862-7463  
John.Dandrea@dbr.com

Jeffrey T. Ganiban  
(202) 230-5150  
Jeffrey.Ganiban@dbr.com

Stephanie Dodge Gournis  
(312) 569-1327  
Stephanie.DodgeGournis@dbr.com

Jeanna Palmer Gunville  
(312) 569-1261  
Jeanna.Gunville@dbr.com

Kelley Taylor Hearne  
(202) 230-5127  
Kelley.Hearne@dbr.com

Kristy M. Hlavenka  
(973) 549-7115  
Kristy.Hlavenka@dbr.com

Todd D. Johnston  
(609) 716-6674  
Todd.Johnston@dbr.com

George H. Kendall  
(973) 549-7070  
George.Kendall@dbr.com

Robert W. McCann  
(202) 230-5149  
Robert.McCann@dbr.com

Gerald P. McCartin  
(202) 230-5113  
Gerald.McCartin@dbr.com

Linda S. Moroney  
(414) 221-6057  
Linda.Moroney@dbr.com

Mark D. Nelson  
(312) 569-1326  
Mark.Nelson@dbr.com

Erin Norby  
(312) 569-1260  
Erin.Norby@dbr.com

Neil S. Olderman  
(312) 569-1279  
Neil.Olderman@dbr.com

Colleen O. Patzer  
(414) 221-6058  
Colleen.Patzer@dbr.com

Kenneth C. Robbins  
(312) 569-1271  
Kenneth.Robbins@dbr.com

Julie M. Rusczek  
(414) 221-6060  
Julie.Rusczek@dbr.com

Sara H. Shanti  
(312) 569-1258  
Sara.Shanti@dbr.com

Robyn S. Shapiro  
(414) 221-6056  
Robyn.Shapiro@dbr.com

K. Bruce Stickler  
(312) 569-1325  
Bruce.Stickler@dbr.com

T.J. Sullivan  
(202) 230-5157  
TJ.Sullivan@dbr.com

Douglas B. Swill  
(312) 569-1270  
Douglas.Swill@dbr.com

Leslie M. Tector  
(414) 221-6055  
Leslie.Tector@dbr.com

Jesse A. Witten  
(202) 230-5146  
Jesse.Witten@dbr.com

Fatema Zanzi  
(312) 569-1285  
Fatema.Zanzi@dbr.com