BNA's
Health Law Reporter™

HHS Enforcement

HIPAA Audits

HIPAA Compliance Audits and Heightened Enforcement Are Coming: Are You Ready?

BY MICHAEL A. DOWELL

The Health and Human Services (HHS) Office of Civil Rights (OCR) recently awarded Booz Allen Hamilton a contract for Health Insurance Portability and Accountability Act (HIPAA) audit candidate identification,[1] and named KPMG as the recipient of a contract to develop a HIPAA auditing protocol and conduct audits on 150 covered entities and business associates before Dec. 31, 2012.[2] The recent contracts are consistent with OCR's intention of increased enforcement activities under the HITECH Act.

HIPAA Enforcement and Audits Required by the HITECH Act.

''There will be enforcement consequences for failure to comply with HIPAA privacy and security obligations,'' according to Susan McAndrew, OCR's Deputy Director for Health Information Privacy.[3]

Generally, OCR has initiated investigations of possible HIPAA violations based on complaints that it has received, and OCR has conducted a limited number of compliance reviews of covered entities. Section 13411 of the Health Information Technology for Economic and Clinical Health (HITECH) Act required HHS to conduct periodic audits of providers and business associates to ensure their compliance with ''this subtitle and subparts C and E of part 164 of title 45, Code of Federal

[1] http://op.bna.com/pl.nsf/r?Open=byul-8klmkn.

[2] http://op.bna.com/pl.nsf/r?Open=byul-8klmml.

[3] ''OCR's McAndrew on HIPAA Enforcement: There Will Be Consequences for HIPAA Violations,'' Howard Anderson, Executive Editor, HealthcareInfoSecucrity.com, Interview with Susan McAndrew (April 13, 2011) http://www.healthcareinfosecurity.com/articles.php?art_id=3537.

Regulations, as such provisions are in effect as of the date of'' the HITECH Act.[4]

Section 13410(e) of HITECH authorizes state attorneys general to bring HIPAA enforcement actions in federal court, as *parens patriae*, on behalf of state residents threatened or affected by a violation of HIPAA. OCR recently provided HIPAA enforcement training for attorneys general and their staff in four regional meetings from April through June of this year. OCR paid all expenses for two members of each state's attorney general's office to attend the two-day meetings, with the goal and objective of ensuring ''that state attorneys general will be better prepared to carry out their new authority under the HITECH Act in enforcing HIPAA.''[5]

Identification of HIPAA Audit Candidates

Booz Allen Hamilton will conduct the ''audit candidate identification'' intended to identify the universe of covered entities and business associates subject to potential audit. The sizes and types of entities selected for audit will vary, and the criteria for selection have not been disclosed. McAndrew has discussed the OCR audits in recent presentations, stating that ''OCR has not determined whether it will audit business associates in addition to covered entities.''[6] When asked who would be audited, McAndrew provided the following insightful points:

> ''We will be looking for meaningful ways of targeting the audit [candidate] selections . . . true to the typical audit protocols. . . . It will not be totally random . . . but this [audit program] will not be incident-driven, unlike the current investigations and compliance reviews that we do. This is an opportunity for us to select on a more random basis who we will be looking at. OCR will provide advance notice to entities selected for the audit process, and make advance requests for documentation.''[7]

Scope and Process of HIPAA Audits

The OCR HIPAA audit contract solicitation indicated that required audit work will include a site visit, including:

- interviews with leadership (e.g., chief information officer, privacy officer, legal counsel, health information management/medical records director);
- examination of physical features and operations;
- consistency of process to policy; and
- observation of compliance with regulatory requirements.[8]

McAndrew says the audit program will occur in three steps. OCR will work with KPMG to develop a comprehensive set of protocols for how audits will be conducted and what measures will be used to evaluate compliance. Then OCR will do an initial round of up to 20 audits to field test the program. If the test audits return positive results, OCR will launch a full range of onsite audits and an evaluation process. ''Audits initially likely will offer comprehensive assessments of compliance with the HIPAA privacy and security rules, rather than focusing on specific narrower issues.''[9]

Audit Reporting Requirements

The results of an audit will be communicated to covered entities in a manner that will consist of an initial audit report containing the auditors' findings and a required plan of correction for any deficiencies, followed by a final report. The auditors will be required to prepare a preliminary written report of the audit, consisting of:

- the audit timeline and methodology
- best practices noted
- raw data collection materials (including interview notes and completed checklists)
- a certification the audit is complete
- ''specific recommendations'' for actions the audited entity may take to address identified compliance problems ''through a corrective action plan''
- recommendations to the COTR (Contracting Officers' Technical Representative) regarding continued need for corrective action, if any; and
- a description of future oversight recommendations.[10]

Preliminary written reports will likely be shared with the organization upon completion and responses will be incorporated in the Final Audit Report. The ''Final Audit Report must contain an identification and description of the audited entity; the methods used to conduct the audit; acknowledgement of any best practice(s) or success(es); and an overall conclusion. For each finding, the Final Audit Report must provide:

- Condition: the defect or noncompliance observed, and the evidence of each.
- Criteria: a clear demonstration that the negative finding is a potential violation of the Privacy or Security Rules, with relevant citations.
- Cause: the reason the identified noncompliance exists, and an identification of the supporting documentation demonstrating it exists.
- Effect: the risk caused by the identified potential noncompliance.
- Recommendations to correct negative findings.
- Corrective actions taken (if any).''

OCR has not determined whether it will publish individual audit reports or summary reports on trends identified in all of the audits.[11]

UCLA Health System Compliance Resolution Agreement

On July 7, 2011, OCR announced a resolution agreement with the University of California at Los Angeles Health System (UCLA) for potential violations of the

[4] The HITECH Act was passed into law as Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA) (Pub. L. 111-5).

[5] All Signs Point To Ramped Up HIPAA Enforcement. *See* http://op.bna.com/hl.nsf/r?Open=byul-8kspx8.

[6] ''HIPAA Compliance Audits Described: KPMG to Launch Program After Tests,'' Interview with Susan McAndrews, Healthcare Information Security (August 4, 2011); http://www.healthcareinfosecurity.com/articles.php?art_id=3924&opg=1

[7] *Id.*

[8] OCR HIPAA Audit Protocol and Program Performance, Contract Solicitation Number OS57605, Department of Health and Human Services, *see* http://op.bna.com/hl.nsf/r?Open=psts-8ktp64.

[9] Note 13, *supra*.

[10] Note 15, *supra*.

[11] *Id.*

  HLR ISSN 1064-2137

Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules.[12] UCLA agreed to pay $865,500 and enter into a three-year corrective action plan (CAP) to resolve the OCR investigation.[13]

The UCLA resolution agreement involved OCR's findings related to two separate complaints concerning celebrity patients, alleging that unauthorized UCLA employees repeatedly accessed the patients' electronic protected health information (PHI). OCR concluded that numerous UCLA employees repeatedly and without a permissible reason examined the ePHI of many patients, and that during the period in question, UCLA did not provide and/or did not document the provision of necessary and appropriate Privacy and Security Rule training to all workforce members. OCR further concluded that UCLA failed to sanction and/or document sanctions of employees who impermissibly examined the patients' PHI, and failed to implement security measures sufficient to reduce the risks of impermissible access to ePHI by authorized users to a reasonable and appropriate level.[14]

As the result of OCR's findings, UCLA was required to agree to the broadest corrective action plan to date that OCR has required of any covered entity. The UCLA corrective action plan requires the covered entity to address the following issues:

Policies and Procedures

UCLA must review, revise and maintain existing policies and procedures and develop, implement and maintain written policies and procedures that comply with federal standards that govern the privacy and security of PHI. It must provide such policies and procedures to HHS within 60 days for review and approval and will have 60 days to implement such policies and procedures following receipt of HHS approval. UCLA must distribute policies and procedures to all applicable workforce members within 30 days of HHS approval and to new members within 30 days of their start date, require signed written or electronic initial compliance certification for all applicable workforce members (that they have read, understand, know where to seek information and will abide by such policies and procedures) that must be submitted to covered entity designees within 30 days of PnP distribution. UCLA is required to assess, update and revise as necessary policies and procedures at least annually and more frequently if appropriate, distributing to and receiving new compliance certifications from all applicable workforce members within 30 days of the effective date of any approved substantive revisions.[15]

Training

All UCLA workforce members must receive specific training related to policies and procedures within 90 days of implementation or within 30 days of their beginning as a workforce member. Each workforce member required to attend training must certify, in writing or in electronic form, that required training has been received and the date of that training. All course materials must be retained, and UCLA must review training annually and update to reflect changes in federal law or HHS guidance, any issues discovered during audits or reviews, or any other relevant developments. UCLA is required to prohibit any workforce member from accessing PHI if requisite training has not been completed.[16]

Monitoring

UCLA is required to designate an Independent Monitor within 90 days to review compliance with the CAP. An Independent Monitor Plan must be submitted to OCR describing with adequate detail the plan for fulfilling the duties of the Monitor, and it must be reviewed at least annually. Revisions must be provided to OCR within 10 business days and they must be approved by OCR. The Monitor reviews must investigate, assess, and make specific determinations about UCLA compliance with the CAP requirements, including unannounced site visits at least two times a year, interviews with staff and business associates and follow up on noncompliance reports. The Monitor must prepare a semi-annual report based on reviews and provide such to HHS and UCLA. UCLA must prepare a response to the report and provide the response to HHS. The Monitor must immediately report any significant violations of the CAP to HHS and UCLA and UCLA must prepare a response including a correction plan and provide such to HHS within 10 days of receiving Monitor's report of a significant violation. In the event HHS has reason to believe that the Monitor reviews or reports fail to conform to the CAP requirements or the Monitor reports are inaccurate, HHS may at its sole discretion conduct its own review to determine the accuracy of the Monitor review or reports.[17]

Implementation Report and Annual Reports

UCLA is required to submit written reports to HHS and the Monitor summarizing the status of its implementation of the requirements of this CAP within 120 days of receipt of HHS' approval of the policies and procedures, including an attestation signed by a covered entity (CE) officer; include a copy of all training materials, including an attestation signed by a CE officer that training has been completed and certifications received; include an engagement letter with the Monitor with a summary description of all engagements including any outside financial audits, compliance program engagements or reimbursement consulting and the proposed start and completion dates of the first Monitor review; include a certification from the Monitor regarding its independence from CE; include an attestation signed by a CE officer listing all CE locations and attesting each location is in compliance with CAP obligations; include an attestation signed by a CE officer that the Implementation Report is accurate and truthful; and for each one-year period CE shall submit to HHS and the Monitor Annual Reports with respect to the status of and findings regarding the covered entity compliance with this CAP no later than 90 days after each reporting period.[18]

[12] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/UCLAHSracap.pdf.
[13] *Id.*
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] *Id.*
[18] *Id.*

Lessons Learned From the UCLA Resolution Agreement

Internal access controls regarding patient PHI are important. Workforce access to patient ePHI must be limited to job-related need to access the data. Celebrity patient PHI is a high risk area for CEs and business associates. Covered entities and business associates are expected to prepare for and develop adequate PHI safeguards related to celebrity patient PHI. Covered entities and business associates should:

- actively monitor access to the ePHI of CE celebrity patients
- implement security controls to reduce the risk of impermissible access
- document the provision of necessary and appropriate Privacy and/or Security Rule training on an annual basis for all workforce members
- have vigilant implementation of policies and procedures
- apply appropriate sanctions and/or document sanctions on workforce members who impermissibly examine ePHI; and
- implement security measures sufficient to reduce the risks of impermissible access to celebrity patient ePHI by unauthorized users to a reasonable and appropriate level.

Conclusion

The UCLA Health System resolution agreement is the third major enforcement action taken by OCR in 2011 and brings the total 2011 settlement amounts to nearly $6.2 million, which exceeds the pre-2011 number of resolution agreements and settlement amounts. OCR's 2011 enforcement actions signal the government's aggressive enforcement intentions for 2011 and thereafter. Corrective action plans, such as the one imposed upon UCLA, can subject a covered entity to significant compliance monitoring obligations, and the requisite costs and expenses related thereto.

The new audits will expand OCR's activities in compliance enforcement. Entities that are found to be substantially out of compliance are likely to be further investigated and subject to fines, penalties, and required to enter into Corrective Action Plans. Providers should take steps to prepare now to avoid becoming the target of an audit or investigation.

Covered entities and business associates should begin by reviewing their current level of compliance and updating their risk assessment. Policies, procedures and training materials should be reviewed and updated to reflect changes in operations, new technology (e.g. electronic health records), and to incorporate changes required by modified provisions of the HIPAA Privacy and Security regulations. HIPAA auditors are likely to carefully review how HIPAA policies and procedures have been developed, documented, implemented, communicated, enforced, and how effective they have been.

Covered entities and business associates should confirm that internal policies and procedures reflect actual practices, and that the HIPAA compliance program is effectively working. A comprehensive audit will identify areas that may require policy or procedural changes, and ensure optimal HIPAA compliance. There should be written reasonable explanations for not implementing any addressable HIPAA security requirements, and documentation of all HIPAA compliance management efforts.

HLR ISSN 1064-2137

HLR ISSN 1064-2137