HALL RENDER
KILLIAN HEATH & LYMAN

HEALTH LAW NEWS

JUNE 13, 2012

OCR PROVIDES UPDATE ON HIPAA SECURITY AND PRIVACY AUDIT PROGRAM

The second wave of the HIPAA Security and Privacy Audit Program conducted by the HHS Office for Civil Rights (OCR) is underway. Linda Sanches, the Lead for HIPAA Compliance Audits for the OCR, provided a detailed update on the Audit Program at the fifth annual *Safeguarding Health Information: Building Assurance through HIPAA Security* conference held last week in Washington, D.C. This conference is co-hosted by OCR and The National Institute of Standards and Technology (NIST) and was attended by health care industry participants, including attorneys from Hall Render.

HIPAA AUDIT PROGRAM OVERVIEW

The Audit Program is part of an HHS initiative to assess HIPAA compliance by covered entities, identify best practices and discover previously unknown risks, weaknesses and vulnerabilities. The initial Audit Program notification and its characteristics were previously described in Hall Render's *HIPAA goes HITECH Impact Series* article available here.

UPDATE: ENTITIES SELECTED FOR AUDIT

Ms. Sanches stated that a sample of 115 covered entities has been chosen for the HIPAA Audit Program from a pool of 3.3 million covered entities. To ensure a wide variety of entities were represented in the audit, selection criteria was based on various factors that include public/private status, the covered entity's size (revenues, number of beds, employees), affiliation with other health care organizations, geographic location and an entity's relationship to patient care. Business associates will be included in future audit programs.

WAVE 1 AUDITS

The first wave of the Audit Program included 20 covered entities (10 providers, 8 health plans and 2 clearinghouses) divided into four different groupings: Level 1 entities (large provider or plan with $1 billion or more in revenues that use HIT extensively), Level 2 entities (regional providers or plans with revenues between $300 million to $1 billion with paper and HIT enabled workflows), Level 3 entities (community hospitals, regional pharmacies, self-insured health plans that do not adjudicate their own plans with $50-300 million in revenues that use some HIT) and Level 4 entities (small providers, community hospitals or rural pharmacy with revenues less than $50 million and little to no use of HIT - almost exclusively paper-based workflows). It is interesting to note that self-insured health plans were chosen among these covered entities, including employer-sponsored health plans of businesses unrelated to the health care industry.

WAVE 2 AND 3 AUDITS

Ms. Sanches reported that the second wave of audits is already underway; 25 letters have been issued to new auditees, and the auditors are currently in the field. OCR anticipates another 70 letters going out to covered entities, with the goal of completing a total of 115 audits by the end of 2012.

INITIAL AUDIT FINDINGS

Ms. Sanches also provided some insight regarding the findings as a result of the first 20 audits. These findings were described in summary fashion, categorized by covered entities, privacy and security issues and policies/procedures. We noted that the majority of findings involved HIPAA Security Rule requirements rather than Privacy Rule requirements. The deficiencies identified in the first 20 audits included contingency planning and user activity monitoring, among many others. Interestingly, the majority of deficiencies involved the Level 4 provider entities.

OCR ENFORCEMENT, ASSISTANCE AND REGULATORY ACTIVITY

The Audit Program is one of several new OCR activities devoted to HIPAA compliance. In Ms. Sanches' presentation at the conference, she noted that the Audit Program is intended to serve as a compliance improvement tool rather than an enforcement tool. An audit may uncover vulnerabilities and weaknesses that can be appropriately addressed through voluntary corrective action on the part of the covered entity. While this may bring some comfort to the covered entities selected for audit, Ms. Sanches reminded the audience that if an audit indicates serious compliance issues, it may trigger a separate enforcement investigation by OCR.

Leon Rodriguez, Director of OCR, also presented at the OCR/NIST conference. He stated that OCR's tolerance for noncompliance is decreasing and increased enforcement efforts will continue. More technical assistance will be offered to small providers, as well as other guidance for the industry. Mr. Rodriguez also announced that he expects the HITECH "Omnibus Rule" amending several HIPAA Security and Privacy Rule provisions to be issued "very soon."

IF YOU RECEIVE AN AUDIT PROGRAM LETTER

It is important that covered entities respond appropriately if a letter is received from OCR or its agents regarding inclusion in the HIPAA Audit Program. OCR requires all responsive documents be provided within 15 business days of an audit request. More information about the Audit Program can be found at the HHS/OCR HIPAA Privacy & Security Audit Program Site at http://www.hhs.gov/ocr/privacy/index.html.

Hall Render's HIPAA microsite, intended to be a single comprehensive resource for tracking various HIPAA-related regulatory developments, analysis and practical guidance, can be accessed at http://www.hallrender.com/hipaa/.

If you have any questions or concerns regarding the HIPAA Security & Privacy Audit Program, please feel free to contact Elizabeth Callahan-Morris or Margaret Marchak at (248) 740-7505, or by email at ecallahan@hallrender.com or mmarchak@hallrender.com, or your regular Hall Render attorney.