Assessments from the Assessor Perspective

Monday, May 18, 2009

Brian C. Johnson, CPA.CITP, CISA
Audit Manager
HHS-OIG-OAS

Agenda

- What We've Done
- Where We Are in the Process
- What We Found
- What We Plan To Do in the Future

What We've Done

- We conducted a series of audits nationwide designed to determine the extent and effectiveness of CMS's oversight and enforcement of the HIPAA Security Rule

What We've Done

- We selected eight hospitals located nationwide with the largest total Medicare billings in fiscal year 2006 (more than $150 million).

What We've Done
Objective

- Our objective for the nationwide hospital audits was to test whether they had implemented certain technical, physical, and administrative safeguard provisions of the HIPAA Security Rule.

What We've Done
Criteria

- The HIPAA Security Rule requires a covered entity, such as a health plan or health care provider that transmits any health information in electronic form, to (1) ensure the integrity and confidentiality of the information, (2) protect against any reasonably anticipated threats or risks to the security or integrity of the information, and (3) protect against unauthorized uses or disclosures of the information.

What We've Done
Criteria (Cont.)

Security Guides and Manuals References in the OIG Reports			
Ref #	**Reference**	**Category**	**Freq.**
4	NIST 800-12 The NIST Handbook, Intro to Computer Security	AC	95
1	OMB Circular A-130, Appendix III	SP	43
L	Local Standard or Procedure	All	33
2	NIST 800-14 Generally Accepted Policies and Procedures	SP	23
8	Federal Information System Controls Audit Manual (FISCAM)	CC	15
5	Federal Information Processing Standards (FIPS) Publication 112 (withdrawn 2/05)	AC	12
19	NIST 800-18, Guide for Developing Security Plans for Information Technology Systems	SP	8
14	NIST 800-34 Contingency Planning Guide	SC	6
13	1999 CFR Title 45 Section 95.621	SP	4
9	Federal Information Processing Standards (FIPS) Publication 87	SC	3
12	NIST 800-48 Wireless Network Security	AC	3
16	NIST 800-40, "Procedures for Handling Security Patches	CC	3
3	Security Awareness Act of 1987, Section 5	SP	2
7	NIST 500-153 Guide to Auditing for Controls and Security	CC	2
10	CMS Business Partners Systems Security Manual	SD	2
11	HHS Automated Information System Security Program Handbook 2.0	SC	2
26	45 CFR, Part 95, Subpart F § 95.621	SP	2

What We've Done
Review Focus Areas

- HIPAA Security Rule Technical Safeguards
  - Access Controls
  - Audit Controls
  - Integrity
  - Person and Entity Authentication
  - Transmission Security
- Supplemental Windows, UNIX/Linux, Novell, and Network Controls

What We've Done
Review Focus Areas (Cont.)

- HIPAA Security Rule Physical Safeguards (Limited)
  - Physical Access to computer Resources
  - Legitimate Need for Access
  - Visitors are Controlled
  - Media and Device Back up

What We've Done
Review Focus Areas (Cont.)

- HIPAA Security Rule Administrative Safeguards (Limited)
  - Risk Management
  - Security Incident Procedures
  - Contingency Planning
  - Business Associate Contracts

What We've Done
Tools & Techniques

- The following tools and techniques helped us assess system and network security:
  - NIPPER Network Parser
  - AirMagnet
  - DumpSec
  - We also assessed the access, audit, transmission, and encryption controls of servers hosting and transmitting ePHI data.

Where We Are In The Process

- The nationwide audit is in process
- We have found the following to date:
  - 176 = Number of Findings
  - 22 = Average findings per Hospital
  - 9 to 40 = Range of Findings per Hospital
  - 149 (85 %) = Potential High Impact Vulnerability*

Where We Are In The Process
What We Found

- 84 percent of the findings were in the following HIPAA Security Rule Safeguard Areas:
  - 44 (25 %) = Access Control
  - 27 (15 %) = Transmission Security
  - 22 (13 %) = Integrity Control
  - 19 (11 %) = Wireless Access*
  - 14 (8 %) = Facility Access
  - 12 (7 %) = Audit Control
  - 10 (6 %) = Person/Entity Authentication

What We Plan To Do in the Future

- Consolidate the nationwide hospital results into a roll-up report to CMS

- We would like to use the experience gained and our resources to influence increased protection of electronic protected health information, including electronic health records, by performing independent audits on covered entities and business associates.