12th National HIPAA Summit – Managing a Data Security Audit Program

2.05, 1:15 PM

Chris Apgar, CISSP

Apgar & Associates, LLC

Overview

- HIPAA Data Security Requirements
- Determining Audit Needs
- Developing an Effective Audit Program
- Developing a Plan for Implementation
- Implementing Your Audit Program
- An Audit within an Audit (or Specific Versus General Audits)
- The Need for a Solid Foundation

Introduction

- Presentation follows Data Security Audit Chapter handout
- Can substitute “privacy” for “data security”
- Adaptable to small, medium & large organizations
- Meets HIPAA security audit requirement
- Cost in dollars and resources depends on size and complexity of organization

HIPAA Security Requirements

- Security rule requires organizations, at a minimum, to conduct periodic internal audits
- Often advisable to seek an external review or audit (not required by rule)
- Generally determined by the size of the organization, line of business, and, sometimes, contract requirements *(*i.e., Medicare, Medicaid, etc.). Purpose behind audit to determine if an organization has properly documented data security practices, policies, and procedures and meets the requirements of the rule.
- Internal audit defines process of determining an organization's compliance

HIPAA Security Requirements

- To support such an audit the rule describes what needs to be maintained to support such an audit.
- Security rule requires covered entities establish audit controls that record and examine activity in information systems that contain electronic PHI
- Audit controls also are a required technical safeguard in §164.312 of the final HIPAA data security rule.
- It is important to remember that, while HIPAA mandates audit-related activity, data security, as with financial audits, represents sound business practice
- Organizations need to take heed of regulatory requirements, but such requirements need to be viewed in the context of your organization’s culture and business needs. In other words, regulatory requirements need to be heeded, but if they are not viewed in the business context and are taken too lightly or seriously, the organization is adversely impacted

Determine Audit Needs

- Conduct a risk assessment (see pages 7 & 8 of Data Security Chapter for sample form)
- Determine business activities involving PHI or other proprietary information
- Assess audit capabilities (audit logs, paper trails, etc.)
- Assess size and complexity of organization
- Assess legal and business requirements

Developing an Effective Audit Program

- Evaluate risk assessment results
- Form project team to evaluate data gathered and develop organized plan with regular schedule to conduct audits
- Requires defining what looking for, evaluation of activity in conjunction with policies and procedures, evaluate technical infrastructure (see pages 10 through 13 of Data Security Audit Chapter)
- Requires developing standard audit reporting documentation

Developing an Effective Audit Program

- Be sure to evaluate business processes in addition to applications, data storage and transmission
- Evaluate teleworkers/remote users; represents added risk and additional area to audit
- Develop audit handbook defining what will be examined (i.e., data, applications, remote users, etc.)

Developing an Effective Audit Program

- Designate auditor or audit team (preferably outside of information technology (IT) department)
- Work with business to assess if audit program is thorough enough and doesn’t interfere with business processes
- Define audit schedule and what will be done with results

Developing an Effective Audit Program

- Effective audit program only as good as actions taken on findings (i.e., implementing new security practices, modifying policies & procedures, implementing staff training, etc.)
- Need to accommodate legacy systems or applications where vendors have not provided adequate audit trails
- Validate complete audit program using external resources, trade journals, NIST (http://www.nist.gov), other organizations in same business similar in size and complexity

Developing Implementation Plan

- Complete risk assessment and gap analysis.
- Review existing industry standards and develop or amend existing processes and policies to support sound data security practices.
- Review existing industry-specific audit criteria and determine appropriate criteria for your organization.
- Develop related training programs (general and targeted) and a training schedule. (This should not be a one-time event.)
- Implement training programs, including the communication of established audit criteria.

Developing Implementation Plan

- Develop an audit schedule or schedules. (There may be a need to conduct a general audit annually but targeted audits at more frequent intervals.)
- Develop documentation identifying the relative weights associated with audit criteria (i.e., it is more important to address a potential audit finding that indicates the organization’s web site is vulnerable to penetration versus a password problem with one device that is not used to store sensitive information).
- Develop templates for communicating audit findings and suggested solutions to problems identified through the audit process.
- Develop a process for findings follow-up (i.e., following through with responsible management, tracking findings and implemented solutions, etc.).

Developing Implementation Plan

- Communicate the audit schedule to affected management and staff.
- Implement a structured audit program.
- Conduct audits according to the established schedule and communicate findings in an established fashion.
- Schedule a review of the audit process following a complete cycle to evaluate the effectiveness of the audit program.

Developing Implementation Plan

- Involvement of senior management critical
- Need legal and compliance buy in
- Presentation to senior management should include program documentation, overview of legal/regulatory requirements, cost (financial & human resources) and ROI (ROI in this case more of selling the program as an insurance policy)
- Requires staff buy in – not designed to “look over your shoulder”

Implementing Your Audit Program

- Make sure training is complete (staff, IS staff assigned to gather data and auditor or audit team)
- Know audit program must be flexible in the beginning and as the business changes
- React to audit findings in a timely manner
- Make sure sanction policies are up to date to address security violations if found and related to workforce member's actions or inactions

Implementing Your Audit Program

- Create an atmosphere where audit program seen as a benefit and not as a method of penalizing workforce members
- Adhere to processes established and evaluate
- Clearly define audit finding retention period (good idea to keep at least summary reports for six years)
- Incorporate regular risk assessments as part of audit process

Implementing Your Audit Program

- Advantages and disadvantages to internal audit staff
- Advantages and disadvantages to external audit staff
- Importance of continuous training
- Advantages of CISA certified internal auditor

Audit Program Requirements

- Program management responsibility
- Audit criteria review and revision schedule
- Refresher and new employee training process
- Audit process (the detailed procedures) review and revision schedule
- Audit finding follow-up and escalation process
- Individual or day-to-day mini-audit processes and management
- Regulatory/accreditation compliance requirements and continuous review process

An Audit Within an Audit

- See pages 27 through 29 in the Data Security Audit Chapter
- Specialized audits versus general audits
- Mini audits or auditing hardware, software, databases, etc. versus conducting a general audit program
- Need to supply information from mini audits to auditor or audit team

An Audit Within an Audit

- Examples:
  - Firewall audit
  - Web site security audit (especially secure web sites open to the public, patients or health plan members)
  - Operating system audits
  - Application specific audits
  - Wireless network security audit
  - Remote user access audit

References

- Data Security Audit Chapter
- NIST – http://www.nist.gov
- WEDI – http://www.wedi.org
- ISACA (CISA certification) - http://www.isaca.org/template.cfm?section=home
- SecurityMetrics (3rd party auditors) - http://www.securitymetrics.com/consulting.adp

References

- Green Pages (3rd party audit) - http://www.greenpages.com/it_solutions/it-audits.asp?gclid=CK_s6qir0IMCFQ2hSQod1i257w
- ISO 1799 Security Audit Tool – http://praxiom.com/iso-17799-audit.htm
- CyberGuard – http://www.cyberguard.com/news_room/Security_Articles/Implementing_IS.html?lang=de_EN
- ISACA San Francisco Generic Audit Manual - http://www.sfisaca.org/resources/genaudpgm.htm
- Medical University of South Carolina Security & Audit Policies - http://www.musc.edu/security/policy/audit-controls.shtml

Q&A

Chris Apgar, CISSP
President
Apgar & Associates, LLC
10730 SW 62nd Place
Portland, OR 97219
(503) 977-9432 (voice)
(503) 816-8555 (mobile)
Capgar@easystreet.com