Health Care Compliance Group

EVALUATING YOUR INFORMATION SECURITY PROGRAM

The Eighteenth National HIPAA Summit

February 4, 2010

Angel Hoffman, RN, MSN

Phyllis A. Patrick, MBA, FACHE, CHC

© AP Health Care Compliance Group February 2010

SESSION OBJECTIVES

- Review of the HIPAA Security Rule Requirements
- Regulatory Requirements, including the HITECH Act
- Impact of HITECH on Information Security Programs
- Provide an Evaluation Checklist
- Lessons learned from CMS 2008 Reviews and Audits
- Tools and Resources for Evaluating Your Program
- Best Practices for ongoing Evaluation

© AP Health Care Compliance Group February 2010

Security Rule
Evaluation Standard

Perform a periodic technical and non-technical evaluation, based initially upon the standards and implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity’s security policies and procedures meet the requirements of this subpart.” [§164.308(a)(8)]

© AP Health Care Compliance Group February 2010

Related Standards (REQUIRED)

- Security Management Process §164.308(a)(1)(i)
- Risk Analysis §164.308(a)(1)(ii)(A)
- Risk Management §164.308(a)(1)(ii)(B)
- Information System Activity Review §164.308(a)(1)(ii)(D)

© AP Health Care Compliance Group February 2010

Information Security Program Regulatory Compliance

ASSESSMENT

- How Do You Define Your Organization’s Information Security Program?
- How does Senior Management describe the Program?
- Assess gaps in understanding and philosophies.

Information Security Program Regulatory Requirements

- HIPAA Privacy Rule
- HIPAA Security Rule
- HITECH ACT
- State Security Breach Notification Laws [e.g., Conn. Gen Stat. 36a-701(b)]
- Fair Credit Reporting Act (FCRA) – Sec. 621
- Individual State Laws (e.g., CA, MA)

© AP Health Care Compliance Group February 2010

HITECH

Primary Provisions & Impact on your Program

- Enforcement and penalties based on a tiered system, which determines if violation was due to “willful neglect”
- Individual State Attorney Generals can become involved and levy fines
- Business Associates required to follow administrative, technical and physical safeguards – same responsibility and accountability as Covered Entities
- Business Associates now subject to same civil and criminal penalties, as Covered Entities, for violations

“I see the HITECH ACT providing a completeness to the HIPAA security and privacy building blocks as we move into a more robust e-health environment.” **(John Parmigiani)**

© AP Health Care Compliance Group February 2010

HITECH
BREACH NOTIFICATION RULE

- Must provide notification to affected individuals, the Secretary, and in certain instances, to the media

- Individual Notice of unsecured PHI via first-class mail or alternately by email if individual agrees to receive electronically, and provided no later than 60 days following discovery of the breach

- Notice contains required elements

- If breach affects > 500 individuals in the same state or jurisdiction, Covered Entity required to provide notice to the Secretary within 60 days, as well as through the media, in addition to providing individual notices

- If breach affects < 500 individuals, then Covered Entity may notify the Secretary of such breaches on an annual basis

- Notification to Secretary is via HHS website by completing and electronically submitting a breach report form

© AP Health Care Compliance Group February 2010

HITECH

BURDEN of PROOF

- Covered Entities and Business Associates must demonstrate that all required notifications have been provided or that a use of disclosure of unsecured PHI did not constitute a breach; also requires:
  - Written policies and procedures are in place
  - Must train employees on these policies and procedures
  - Must develop and apply appropriate sanctions against workforce members who do not comply with policies and procedures

- Patient now has the ability to restrict Protected Health Information (PHI), but Covered Entities are not required to comply with the request

- Patients may receive full account of disclosures, including information disclosed for the purpose of treatment, payment and healthcare operations (TPO)

HITECH

IMPORTANT DATES

- ***February 17, 2010:***
  - Determine qualifications of individuals performing review
  - Restrictions on marketing and fundraising take effect
  - Deadline for HHS secretary to issue guidance on how Covered Entities must comply with "de-identification" of PHI, or what limits they have when they use patients' information for research purposes

- ***August 17, 2010:***
  - Deadline for HHS secretary to issue regulations on sale of PHI
  - Comptroller General must submit report to HHS secretary offering recommendations on what a patient harmed by a breach is entitled to in a financial settlement

EVALUATION CHECKLIST:
How Does Your Program Stack Up?

Health Care
Compliance
Group

☑ Do you have a dedicated Security Officer? Reporting relationship?

☑ Where is Security in the organizational chart?

☑ Have you audited compliance with your Privacy and Security Training Programs?

☑ Have you reviewed and/or revised Business Associate Agreements (BAA)?

☑ Do you plan to compare current BAAs with new Privacy and Security requirements and incorporate them into new agreements?

© AP Health Care Compliance Group February 2010

EVALUATION CHECKLIST

Health Care Compliance Group

☑ When did you last conduct a formal evaluation of your program?

☑ How do you define “periodic”?

☑ Did you include both technical and non-technical aspects in your evaluation?

☑ As a result of security moving up on the risk matrix, is risk analysis conducted on an ongoing basis?

☑ Do you integrate Information Security into the organization’s overall risk management and risk analysis program?

© AP Health Care Compliance Group February 2010

EVALUATION CHECKLIST

Health Care Compliance Group

☑ When are policies reviewed at your organization?

- Annually?
- When an issue or an event occurs?
- During or following the implementation of a new system?

☑ Is there existing documentation of your policy review and approval process?

☑ Do you have a process for communicating new and revised policies?

EVALUATION CHECKLIST

☑ Can you prove the existence of a continuing awareness training program for all employees and contractors?

☑ Have you refreshed your security awareness training program since the Security Rule was implemented?

- ✓ Does training occur annually?
- ✓ Is training mandatory?
- ✓ Does Senior Management complete the training?
- ✓ Does the Board participate in training?
- ✓ Does training include contractors and vendors?

EVALUATION CHECKLIST

☑ Are audit procedures followed (for consistency with documented procedures) by:

- ✓ Management?
- ✓ Physicians?
- ✓ Staff?

☑ Is network vulnerability testing conducted on a regular basis?

☑ What is the frequency of vulnerability testing at your organization?

☑ Who is responsible for testing?

© AP Health Care Compliance Group February 2010

EVALUATION CHECKLIST

☑ What mechanisms are in place for evaluating that processes are operating effectively?

☑ Who is involved in the evaluation/audit process?

☑ Is the process performed with internal or external resources?

☑ What is the frequency of evaluations?

☑ Are changes made to the Program, based upon the results?

EVALUATION CHECKLIST

American Recovery and Reinvestment Act (ARRA) & Electronic Health Records (EHRs)

☑ Are periodic audits of information systems activity review, user login monitoring, audit log review, user access controls being conducted?

☑ Have the results of these audits changed your processes?

☑ Are responsibilities for information security processes, mandatory training, etc., incorporated into performance evaluations for all employees?

☑ Are pay increases and bonuses affected by completion of mandatory training and compliance with security processes as documented in performance evaluations?

CMS 2008 COMPLIANCE REVIEWS: LESSONS LEARNED

- On-site reviews, consisting of interviews and document requests, conducted with 8 hospitals and organizations of various sizes
- Results indicated inconsistent practices across organizations
- CEs did not have formalized policy review and approval processes; and did not review and approve security policies within the timeframe required
- Documented procedures were inconsistent with procedures followed by personnel. As processes evolved, documentation did not occur.

- **RESULTS OF IG REVIEW of CMS OVERSIGHT:**
  - More focus on compliance reviews and increased enforcement

LESSONS LEARNED

- The **EVALUATION STANDARD** in the Security Rule emphasizes the importance of **continued effectiveness of security processes driven by documented policies and procedures.**

- Purpose of the Standard is to ensure that Covered Entities continue to comply with the Security Rule and maintain the Confidentiality, Integrity, and Availability (CIA) of ePHI.

TOOLS & RESOURCES

- HIPAA Security Series (CMS)
- NIST 800 Series
  - SP 800 – 37: Guide for the Security Certification and Accreditation of Federal Information Systems
  - SP 800 – 53: Recommended Security Controls for Federal Information Systems
  - SP 800 – 53A: Guide for Assessing the Security Controls in Federal Information Systems
- HIMSS Annual Leadership Surveys
- HIMSS U.S. Healthcare Industry HIPAA Compliance Survey Results
- Vendor Tools and Packages

TOOLS & RESOURCES

Tools and resources may enhance your Program, but …..without a dedicated Security Officer and resources, commitment of senior leadership, a program based on policy and integrated into the culture of the organization, achieving and maintaining Compliance will be a moving target.

- Some commercial tools and products are costly and difficult to use
- Results may vary or be insufficient depending on the tool used
- Ongoing maintenance is costly (people, time, contracts, etc.)

BEST PRACTICES

- Establish a **formal, ongoing Evaluation and Review Process** using independent consultant/third party. Conduct the review using **project management** tools and methods.

- Perform **Risk Analysis**, following established policies and procedures, at a minimum, every three years or whenever there is a significant change in the environment (e.g. , new system, changes in senior management)

- Establish an ongoing **Steering Committee**:
  - Dedicate a multi-disciplinary team responsible for guiding the Evaluation Process
  - Determine level of risk and threat to the organization

BEST PRACTICES

- Retain **independent consultant that meets following criteria:**
  - Determine qualifications of individuals performing review
  - Ask questions to ascertain if consultants possess “hands on” experience
  - Do reports summarize data or provide noted gaps analysis?
  - Does the consultant provide a “to do list” based upon the audit results, mapping a path for the organization to follow or is it buried in the summary?
  - Do you understand the results and have support from the organization to resolve issues identified?

- Elicit **support from senior management** to provide adequate **resources** to address areas of identified risks
  - Organizations that ignore findings are subject to **increased penalties**
  - **Documentation and retention** of action plan and follow-up

Health Care
Compliance
Group

QUESTIONS?

© AP Health Care Compliance Group February 2010

Angel Hoffman

Angel@aphccompliance.com

412-559-6703

Phyllis A. Patrick

Phyllis@aphccompliance.com

914-696-3622