HIPAA Business Associates and Security Risk Analysis

Alan Davis, PMP, GSLC
Principal
Proteus Consulting

Association of Alcoholism and Addiction Programs in Washington State

Experience • Integrity • Results

Legal Disclaimer

Legal Disclaimer. This information does not constitute legal advice and is for educational purposes only. This information is based on current federal law and subject to change based on changes in federal law or subsequent interpretative guidance. Since this information is based on federal law, it must be modified to reflect state law where that state law is more stringent than the federal law or other state law exceptions apply. This information is intended to be a general information resource regarding the matters covered, and may not be tailored to your specific circumstance. YOU SHOULD EVALUATE ALL INFORMATION, OPINIONS AND ADVICE PROVIDED HEREIN IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISOR, AS APPROPRIATE. The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by Proteus Consulting, LLC.

Who Are We?

- Exclusively HIPAA Security Rule Oriented
- Compliance and Security Risk Analysis
- Policies and Procedures
- Workforce Training

What Do We Want to Talk About?

- Business Associates
- HIPAA Security Risk Assessment
- Running a HIPAA Security Program

One Quick Hook…

The Audit Protocol – 2012 vs. 2016

- Inquire of management as to whether formal or informal policy and procedures exist
- Obtain and review formal or informal policy and procedures
- Evaluate the content in relation to the specific performance
- Determine if formal or informal policy and procedure have been approved and updated

- Does the entity have policies and procedures in place?
- Determine how the entity has implemented the requirements
- Obtain and review documentation demonstrating that policies and procedures have been implemented
- Evaluate and determine if practices are handled in accordance with the related policies and procedures

One Quick Hook…
(cont.)

Phase 2 Audits

- 7.11.16: 167 Covered Entities were notified of their selection
- Received two emails
  - Notification, response timeline and OCR online portal link
  - Additional request to provide a BA list and OCR's desk audit process webinar information
- Covered Entities had 10 days (7.22.16) to respond to all document requests

One Chance to Show Compliance!

One Quick Hook…
(cont.)

- Privacy
  - Notice of Privacy Practices and consent requirements
  - Provision of notice
  - Right to access
- Security
  - Risk Analysis
  - Risk Management
- Breach Notification
  - Timeliness of notification
  - Content of notification

This Is You!

Covered Entities

- A Covered Entity (CE) is a:
  - Healthcare Provider: doctors, clinics, psychologists, dentists, chiropractors, nursing homes, pharmacies
  - Health Plan: health insurance companies, HMOs, company health plans, government programs that pay for health care (e.g. Medicare, etc.)
  - Heath Care Clearinghouse: Entities that process non-standard health information
- CEs Must Comply With Requirements to Protect the Privacy and Security of Health Information

Business Associates

- A Business Associate (BA)
  - Is a person who performs a function or activity on behalf of, or provides services to, a Covered Entity or to another BA (i.e. subcontractors) that involves individually identifiable health information
  - Is not a covered entity workforce member
  - Must comply with applicable sections of HIPAA Privacy Rule
  - Must comply with HIPAA Security Rule
  - Must comply with the HIPAA Breach Notification Rule
  - Has direct liability to protect health information

Business Associates
Sharing PHI

- Security Rule §164.314(a)(1 & 2) Applies
  - Business Associate Contracts and Other Arrangements
- Written Executed Contract BEFORE sharing PHI
- Post Contract Due Diligence
- OCR 2016 Protocol and Legal Counsel

Business Associates
Contract Elements

- Establish Permitted and Required Uses and Disclosures
- Provide That BA Will Not Use or Further Disclose Other Than Permitted
- Require BA to Implement Safeguards to Prevent UA or Disclosure
- Require BA Report to CE Other Than Permitted Disclosure

Business Associates
Contract Elements (cont.)

- Require BA Satisfy Obligation for Individual's Request(s)
- Require BA Carry Out Obligations Consistent with CE
- Require BA Make Available Practices, Books & Records to HHS
- Require BA Return or Destroy PHI at End of Contract

Business Associates
Contract Elements (cont.)

- Require BA to Ensure Subcontractors Agree to Same Conditions
- Authorize CE to Terminate Contract if BA Violates Term(s)
- Additionally
  - Indemnity Clause & Breach Notification Responsibilities
  - Define BA Satisfactory Assurances w/o Introducing Agency Relationship
  - Requirement to Develop a Breach Communication Plan Within 30 Days

HIPAA-based Security Risk Analysis
Understanding the Risks

- What's the Risk?
- Health and Human Services / Office of Civil Rights Guidance
- National Institute of Standards and Technology

HIPAA-based Security Risk Analysis
Lifecycle & Methodology

- NIST Methodology (SP 800-30)
  - Scope §164.306(a)
  - Collect Data §164.306(a)
  - Identify Threats and Vulnerabilities §164.306(a)(2)
  - Assess Current Controls §164.306(b)
  - Determine Likelihood §164.306(b)(2)(iv)
  - Determine Impact §164.306(b)(2)(iv)
  - Calculate Risk §164.308(a)(1)(ii)(A)

HIPAA-based Security Risk Analysis
Security Evaluation vs. Risk Analysis

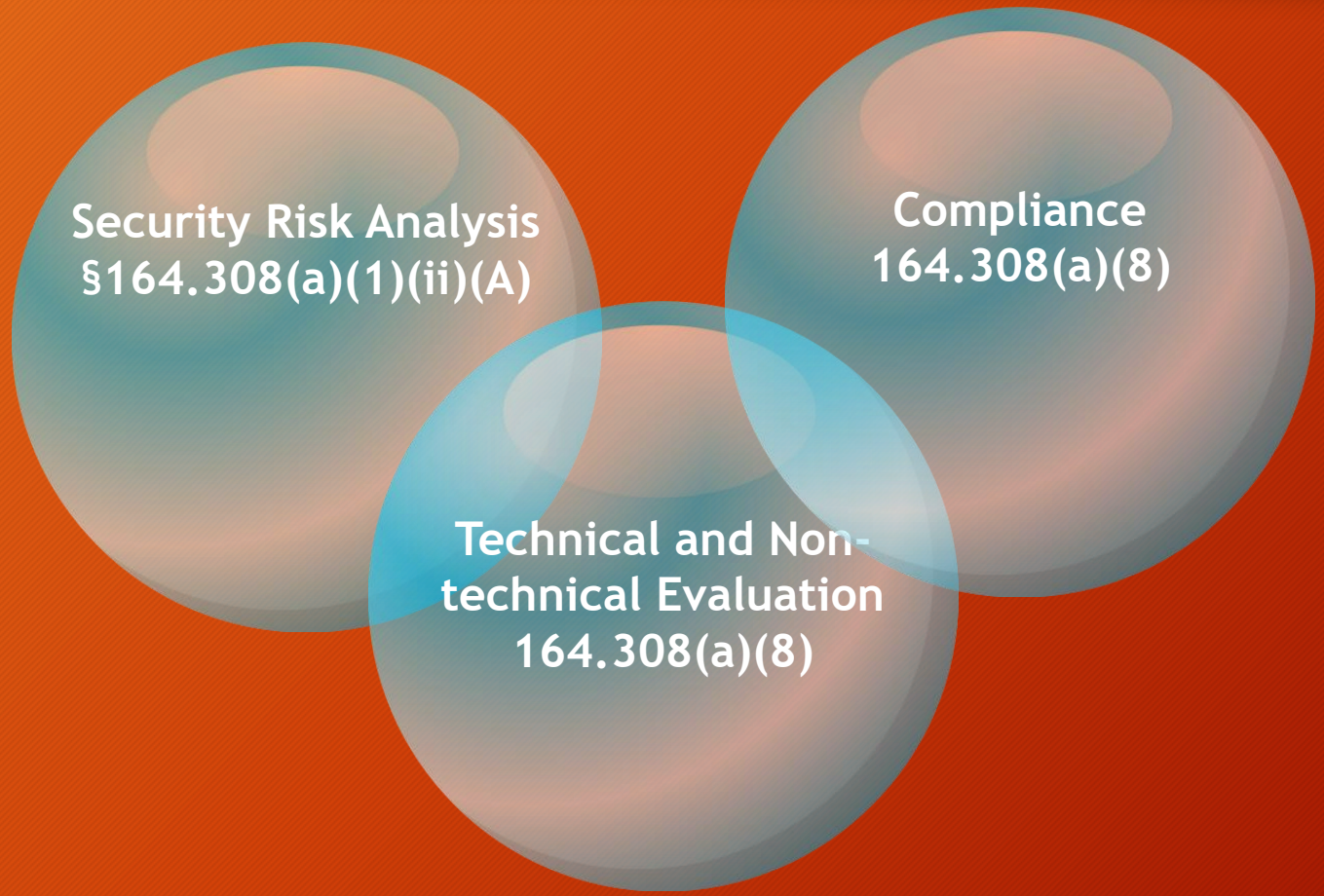
45 CFR §164.308(a)(8) Standard: Evaluation

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

45 CFR. §164.308(a)(1)(i) Standard: Security Management Process

- (1)(i) Standard: Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations.
- (ii) Implementation specifications: (A) Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.

HIPAA-based Security Risk Analysis
Analyzing & Evaluating



HIPAA-based Security Risk Analysis
Tools and Approaches

- Checklists (no!)
- Risk Matrix Spreadsheets
- Office of National Coordinator for Health Information
- Software as a Service (SaaS) Tools

HIPAA-based Security Risk Analysis
Tools and Approaches (cont.)

- Tools vs. Knowledge
- Tips for Seeking Help
- The OCR Protocol
- Risk Analysis Myths

HIPAA-based Security Risk Analysis
Post SRA Action Approach

- Risk Responses
- Document Mitigation Plan Work (Project)
- Policy – Procedure – Training - Practice
- Incorporate into Risk / Quality Program

Your HIPAA Security Program
Visible, Demonstrable Evidence

- Operational and Capital Funding
- Program Sponsorship
- Measures of Effectiveness
- HIPAA Security Officer

Your HIPAA Security Program
Five Challenges

- Understand the Threat Environment
- Sufficient Resources
- Effectively Measure Risks and Processes
- Overcome Information Security Apathy
- Tools to Prevent or Eliminate Threats

HIPAA Security Awareness Maturity Model

Questions or Concerns