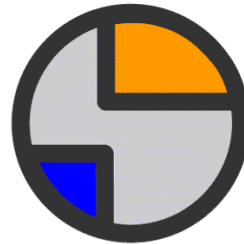


# **HIPAA Security:** *Are You Ready?*

**Tom Walsh, CHS, CISSP**  
President

**Tom Walsh**  
**Consulting, LLC**



# Tom Walsh

- Certified in Healthcare Security (CHS)
- Certified Information Systems Security Professional (CISSP)
- Co-authored a book on HIPAA Security
- Invited speaker at national conferences
- Former information security manager for large healthcare system in Kansas City, MO
- DOE-certified safeguards and security instructor
- A little nerdy, but overall, a nice guy 😊

# Presentation Overview

- Provide examples of indicators that you can use to gauge if you are on the right path toward compliance
- Explain common shortcomings of many healthcare organizations
- Provide practical suggestions for those organizations that are just now starting their security efforts
- Provide an opportunity for attendees to ask their questions at the end of the formal presentation

# #1 Understanding the Rule

- Read the HIPAA Security Rule and the Preamble to gain a full understanding with what is required and why
- Implement reasonable solutions that make good business sense and are based upon organizational risks
  - Protect against any *reasonably anticipated* threats or hazards to the security or integrity of PHI
- National Standards **≠** National Solutions

# #1 Understanding the Rule

## Negative indicators

- ☹ Lacking an understanding of what is truly required by the Rule
- ☹ Treating the Addressable Implementation Specifications as “optional”
- ☹ Failing to see the good business reasons for implementing security –
  - Only doing security for the sake of HIPAA

# #2 Risk Analysis

- Start with your most critical systems
- Determine the ownership for the critical information systems
- Conduct a risk analysis:
  - Identify assets, threats, existing controls, vulnerabilities, likelihood and impacts
- Rate risks accordingly
- Document the findings and recommendations

# #2 Risk Analysis

## Negative indicators

- ☹️ Trying to assess risks to “all” systems that process and store PHI
- ☹️ Purchasing a risk analysis tool to “make it easier”
- ☹️ Failing to include Data Owners in the risk analysis process
- ☹️ Thinking that the organization will only have to do a risk analysis once

# #3 Risk Management

- **Determine the action to be taken regarding the risk:**
  - Mitigation, transference, or acceptance of the risks
- **Apply risk analysis as the rationale for dealing with addressable implementation specifications**
- **Create a budget for security**
  - Acquire needed technology and implementing system “fixes”

# #3 Risk Management

## Negative indicators

- ☹️ Trying to remediate all risks
- ☹️ Failing to document Data Owners or Executive Management's decisions
- ☹️ Creating a remediation plan, but no assignments, due dates, or accountability for completion
- ☹️ Lacking executive support for plans
- ☹️ Looking for a "security-in-a-box" solution

# #4 Assign Responsibility

- Create a job description for the information security officer (ISO)
- Put somebody in charge – appoint an Information Security Officer (ISO)
- Provide high visibility for the position
  - Distribute an executive memo to the entire workforce formally announcing the appointment of the ISO
- Include the ISO's name and contact information as part of the training and awareness

# #4 Assigning Responsibility

## Negative indicators

- ☹️ Allowing other job responsibilities to take precedence over security
- ☹️ Identifying the information security officer – Workforce members are clueless
- ☹️ Having the ISO report too far down in the organization and having no real authority
- ☹️ Lacking separation of duties  
*(Example: CIO is also the ISO)*

# #5 Policies, Procedures, and Plans

- Review current information security policies, procedures, and plans for compliance with HIPAA security
- Create new or update existing policies, procedures, forms, and plans as needed
- Provide easy access to policies
- Enforce policies and apply sanctions

*"If it hasn't been documented, it hasn't been done"!*

# #5 Policies, Procedures, and Plans

## Negative indicators

- ☹ Creating a policy for every standard and every implementation specification

*How many policies do you really need?*

- ☹ Purchasing ready-made HIPAA Security policies, adding the organization's name and considering the job done

# #6 Security Awareness & Training

- Establish a formal information security training program
- Create security awareness that is general for everyone
- Create security training that is specific
- Document audiences, content and delivery methods
  - Syllabus, attendance sheets, handouts, etc.
- Send out periodic reminders

# #6 Security Awareness & Training

## Negative indicators

☹ Looking for a “one size fits all” training solution

Failing to do a “needs assessment”

☹ Allowing some workforce members to skip training

*“I’m an exempt employee, therefore I am exempt from attending training.”*

# #7 Incident Reporting and Response

- Create a process for workforce members to report security incidents
- Create an information security incident report form
  - Or modify an existing privacy or patient occurrence reporting process to now include information security incidents
- Create incident response procedures and an incident response team

# #7 Incident Reporting and Response

## Negative indicators

- ☹ Failing to teach the workforce what is a reportable information security incident
- ☹ Looking to “blame” someone for each incident rather than trying striving for prevention
- ☹ Creating a culture where the workforce fear reporting incidents

# #8 Audits

- Determine user activities and events that should trigger an entry into an audit log
- Perform regular audits:
  - When there is a problem
  - Randomly by user
  - Randomly by patient
- Implement procedures to regularly review and retain audit logs

# #8 Audits

## Negative indicators

- ☹ Failing to predetermine how audits will be conducted
- ☹ Looking at audit logs only when there is a problem
- ☹ Trying to maintain audit logs for six years

# #9 Contingency & Disaster Plans

- Identify the most critical applications and information systems that essential to the organization
- Establish and implement departmental contingency plans and/or procedures for conducting business in response to temporary outages of information systems
- Document data backup plans that outlines the frequency and rotation of backups

# #9 Contingency & Disaster Plans

## Negative indicators

- ☹️ Having a policy that states the organization will have Contingency and Disaster Recovery Plans; but there are no plans
- ☹️ Failing to test and update plans
- ☹️ Thinking, "It will never happen"

# #10 Management Support

- Inform management on the associated risks for operating information systems in their current configuration
- Advise management on cost-effective ways to reduce risks while meeting operational goals
- Provide some cost benefit or return on investment figures for implementing security controls

# #10 Management Support

## Negative indicators

- ☹️ Trying to dictate security to management
- ☹️ Failing to link information security to operational objectives
- ☹️ Having management say, "We don't have to worry about security because we have \_\_\_\_\_ to handle it for us."

# Compliance Program Elements

1. Appointment of an official to oversee the program (Privacy and Security Officer)
2. Set standards of expected conduct (Policies and Procedures)
3. Training, education, and awareness (Training)
4. Process for receiving reports of violations (Incident Reporting)
5. Response to reports (Incident Response)
6. On-going auditing and monitoring for compliance (Audits and Evaluation)
7. Take appropriate corrective actions (Sanctions, risk management, technical security controls)

# Closing Thoughts...

- **HIPAA compliance is not the only driver for security**
- **Information security makes good business sense**
- **Security needs to be implemented based upon risks**
- **Documentation and demonstrated practices along with management support are the best indicators of a real information security program**

# ***Thanks for Participating!***

**Tom Walsh, CHS, CISSP**

**[twalshconsulting@aol.com](mailto:twalshconsulting@aol.com)**

**913-696-1573**

**Tom Walsh  
Consulting, LLC**

