

“Security & Privacy Roundtable: How YOU Doin’ ?”

HIPAA COW Fall 2004 Conference Discussion
October 8, 2004 Wisconsin Dells, WI
Session 2:30-3:30PM

Co-facilitated by:

Lisa Gallagher, BSEE, CISM

Founder/Principal Consultant, Javelin Technology

Former Vice President, URAC Health Information Technology Department

Todd Fitzgerald, CISSP, CISA, CISM

HIPAA COW Board of Directors member, Co-chair Security Taskforce

Director of Systems Security and Systems Security Officer

United Government Services, LLC



Security & Privacy Roundtable: How YOU Doin’? Presented at HIPAA COW Fall 2004 Conference Copyright © 2004 Todd Fitzgerald/Lisa Gallagher All rights reserved. Slide 1

Presenting, Direct from DHHS... The HIPAA Security Rule...

How **YOU** *Doin’?*

Security & Privacy Roundtable: How YOU Doin’? Presented at HIPAA COW Fall 2004 Conference Copyright © 2004 Todd Fitzgerald/Lisa Gallagher All rights reserved. Slide 2

Today's Objectives.. To Share



Security & Privacy Roundtable: How YOU Doin'? Presented at HIPAACOW Fall 2004 Conference Copyright © 2004 Todd Fitzgerald/Lisa Gallagher All rights reserved. Slide 3

HIPAA COW Mission Reminder..

Reduce Duplication

Partner

Assist

Elevate Issues

Share Best Practices

Educate

WWW.HIPACOW.ORG

Security & Privacy Roundtable: How YOU Doin'? Presented at HIPAACOW Fall 2004 Conference Copyright © 2004 Todd Fitzgerald/Lisa Gallagher All rights reserved. Slide 4

Ground Rules For Discussion...



- We have many different payers, providers, clearinghouses coming from different perspectives based upon:
 - size
 - cost/resource constraints
 - technical capabilities
 - geographic locations
 - risk profiles
 - complexity of systems
- All ideas should be respected
- If something has worked for you **please share it**
- If something hasn't worked for you **please share it**

Security & Privacy Roundtable: How YOU Doin'? Presented at HIPAACOW Fall 2004 Conference Copyright © 2004 Todd Fitzgerald/Lisa Gallagher All rights reserved. Slide 5

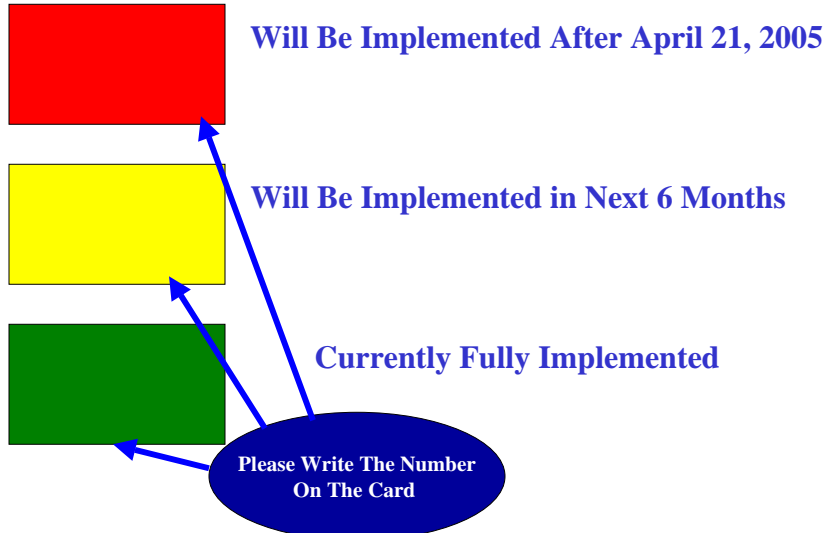
Today's Approach



- Use the NIST Special Publication 800-66 to guide the discussion for each rule
- Discuss Key Activities
- Discuss what has been implemented, how it was approached
 - What worked ?
 - What didn't ?
- Discuss challenges in implementing the rule
- And Finally....

Security & Privacy Roundtable: How YOU Doin'? Presented at HIPAACOW Fall 2004 Conference Copyright © 2004 Todd Fitzgerald/Lisa Gallagher All rights reserved. Slide 6

Where Are You Now (Progress ?)



Security & Privacy Roundtable: How YOU Doin'? Presented at HIPAACOW Fall 2004 Conference Copyright © 2004 Todd Fitzgerald/Lisa Gallagher All rights reserved. Slide 7

1. Security Management Process (§164.308(a)(1))



HIPAA Standard: *Implement policies and procedures to prevent, detect, contain and correct security violations*

Key Activities

- Identify relevant information systems
- Conduct risk assessment
- Acquire IT Systems and services
- Create and deploy policies and procedures

Security & Privacy Roundtable: How YOU Doin'? Presented at HIPAACOW Fall 2004 Conference Copyright © 2004 Todd Fitzgerald/Lisa Gallagher All rights reserved. Slide 8

2. Assigned Security Responsibility (§164.308(a)(2))



HIPAA Standard: *Identify the security official who is responsible for the development and implementation of the policies and procedures required*

Key Activities

- Select a security official to be assigned responsibility for HIPAA security
- Assign and document the individual's responsibility

Security & Privacy Roundtable: How YOU Doin'? Presented at HIPAACOW Fall 2004 Conference Copyright © 2004 Todd Fitzgerald/Lisa Gallagher All rights reserved. Slide 9

3. Workforce Security (§164.308(a)(3))



HIPAA Standard: *Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a) 4 of this section and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to e-phi.*

Key Activities

- Establish clear job descriptions and responsibilities
- Establish criteria and procedures for hiring and assigning tasks
- Establish termination procedures

Security & Privacy Roundtable: How YOU Doin'? Presented at HIPAACOW Fall 2004 Conference Copyright © 2004 Todd Fitzgerald/Lisa Gallagher All rights reserved. Slide 10

4. Information Access Management (§164.308(a)(4))



HIPAA Standard: *Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.*

Key Activities

- Determine criteria for establishing access
- Determine who should be authorized to access information systems
- Evaluate existing security measures related to access controls

Security & Privacy Roundtable: How YOU Doin'? Presented at HIPAACOW Fall 2004 Conference Copyright © 2004 Todd Fitzgerald/Lisa Gallagher All rights reserved. Slide 11

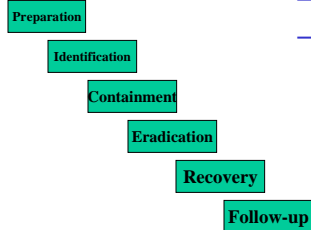
6. Security Incident Procedures (§164.308(a)(6))



HIPAA Standard: *Implement policies and procedures to address security incidents*

Key Activities

- Determine goals of incident response
- Develop and deploy an incident response team
- Develop incident response procedures
- Incorporate post-incident analysis into updates and revisions



Security & Privacy Roundtable: How YOU Doin'? Presented at HIPAACOW Fall 2004 Conference Copyright © 2004 Todd Fitzgerald/Lisa Gallagher All rights reserved. Slide 12

7. Contingency Plan (§164.308(a)(7))



HIPAA Standard: *Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information*

Key Activities

- Develop contingency planning policy
- Conduct an impact analysis (Applications and Data Criticality)
- Identify preventive measures
- Develop recovery strategy
- Develop the contingency plan
- Planning, testing and execution

Security & Privacy Roundtable: How YOU Doin'? Presented at HIPAACOW Fall 2004 Conference Copyright © 2004 Todd Fitzgerald/Lisa Gallagher All rights reserved. Slide 13

8. Evaluation (§164.308(a)(8))



HIPAA Standard: *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 e-phi, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.*

Key Activities

- Determine whether internal or external evaluation is most appropriate
- Develop standards and measurements for all areas and topics of security
- Conduct evaluation
- Document results
- Repeat evaluations periodically

Security & Privacy Roundtable: How YOU Doin'? Presented at HIPAACOW Fall 2004 Conference Copyright © 2004 Todd Fitzgerald/Lisa Gallagher All rights reserved. Slide 14

9. Business Associate Contracts and Other Arrangements (§164.308(b)(1))



HIPAA Standard: *A covered entity, in accordance with Sec 164.306, may permit a business associate to create, receive, maintain, or transmit e-phi on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with Sec. 164.314(a) that the business associate appropriately safeguard the information.*

Key Activities

- Identify entities that are business associates under the HIPAA security rule
- Execute new agreements or update existing agreements as appropriate
- Establish process for measuring contract performance and terminating contract if security requirements are not being met.

Security & Privacy Roundtable: How YOU Doin'? Presented at HIPAACOW Fall 2004 Conference Copyright © 2004 Todd Fitzgerald/Lisa Gallagher All rights reserved. Slide 15

10. Facility Access Controls (§164.310(A)(1))



HIPAA Standard: *Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed (supports IAM Administrative and Access Control Technical standard)*

Key Activities

- Conduct an analysis of existing physical security vulnerabilities
- Identify corrective measures
- Develop a facility security plan
- Develop access control procedures
- Establish contingency operations procedures

Security & Privacy Roundtable: How YOU Doin'? Presented at HIPAACOW Fall 2004 Conference Copyright © 2004 Todd Fitzgerald/Lisa Gallagher All rights reserved. Slide 16

11. Workstation Use (§164.310(b))



HIPAA Standard: *Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.*

Key Activities

- Identify workstation types and functions or uses
- Identify expected performance of each type of workstation
- Analyze physical surroundings for physical attributes

Security & Privacy Roundtable: How YOU Doin'? Presented at HIPAACOW Fall 2004 Conference Copyright © 2004 Todd Fitzgerald/Lisa Gallagher All rights reserved. Slide 17

12. Workstation Security (§164.310(c))



HIPAA Standard: *Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.*

Key Activities

- Identify all methods of physical access to workstations
- Analyze the risk associated with each type of access
- Identify physical safeguards

Security & Privacy Roundtable: How YOU Doin'? Presented at HIPAACOW Fall 2004 Conference Copyright © 2004 Todd Fitzgerald/Lisa Gallagher All rights reserved. Slide 18

13. Device and Media Controls (§164.310(d)(1))



HIPAA Standard: *Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.*

Key Activities

- Evaluate methods for final disposal of electronic health information
- Develop and implement procedures for reuse of electronic media
- Maintain records of hardware, media, and personnel
- Develop backup procedures to ensure that the integrity of electronic health information will not be jeopardized during equipment relocation.

Security & Privacy Roundtable: How YOU Doin'? Presented at HIPAACOW Fall 2004 Conference Copyright © 2004 Todd Fitzgerald/Lisa Gallagher All rights reserved. Slide 19

14. Access Controls (§164.312(a)(1))



HIPAA Standard: *Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in sec 164.308(a)(4). (Supports the IAM Administrative standard and Facilities access controls physical standard).*

Key Activities

- Analyze workloads and operations to identify the access needs of all users
- Identify all data and systems where access control is a requirement
- Ensure that all system users have been assigned a unique identifier

Security & Privacy Roundtable: How YOU Doin'? Presented at HIPAACOW Fall 2004 Conference Copyright © 2004 Todd Fitzgerald/Lisa Gallagher All rights reserved. Slide 20

14. Access Controls (§164.312(a)(1))



Key Activities (Cont'd)

- Develop access control policy
- Implement access control procedures using selected hardware and software
- Review and update user access
- Establish an emergency access procedure
- Terminate access if it is no longer required

Security & Privacy Roundtable: How YOU Doin'? Presented at HIPAACOW Fall 2004 Conference Copyright © 2004 Todd Fitzgerald/Lisa Gallagher All rights reserved. Slide 21

15. Audit Controls (§164.312(b))



HIPAA Standard: *Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.*

Key Activities

- Determine the systems or activities that will be tracked or audited
- Select the tools that will be deployed for auditing and system activity reviews
- Develop and deploy the information system activity review/audit policy
- Develop appropriate standard operating procedures
- Implement the audit/system activity review process

Security & Privacy Roundtable: How YOU Doin'? Presented at HIPAACOW Fall 2004 Conference Copyright © 2004 Todd Fitzgerald/Lisa Gallagher All rights reserved. Slide 22

16. Integrity (§164.312(c)(1))



HIPAA Standard: *Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.*

Key Activities

- Identify all users who have been authorized to access electronic protected health information
- Identify any possible unauthorized sources that may be able to intercept the information and modify it
- Develop the integrity policy and requirements
- Implement procedures to address these requirements
- Establish a monitoring process to assess how the implemented process is working

Security & Privacy Roundtable: How YOU Doin'? Presented at HIPAACOW Fall 2004 Conference Copyright © 2004 Todd Fitzgerald/Lisa Gallagher All rights reserved. Slide 23

17. Person or Entity Authentication (§164.312(d)(8))

LOGIN = HEATHER



LOGIN = HEATHER



HIPAA Standard: *Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.*

Key Activities

- Determine authentication applicability to current systems/applications
- Evaluate authentication options available
- Select and implement authentication option

Security & Privacy Roundtable: How YOU Doin'? Presented at HIPAACOW Fall 2004 Conference Copyright © 2004 Todd Fitzgerald/Lisa Gallagher All rights reserved. Slide 24

18. Transmission Security (§164.312(e)(1))



HIPAA Standard: *Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.*

Key Activities

- Identify any possible unauthorized sources that may be able to intercept and/or modify the information
- Develop a transmission security policy
- Implement procedures for transmitting electronic health information using hardware/software if needed

ILOVETHESECURITYRULE



7F%G34FYNTQD\$X95HDT

Security & Privacy Roundtable: How YOU Doin'? Presented at HIPAACOW Fall 2004 Conference Copyright © 2004 Todd Fitzgerald/Lisa Gallagher All rights reserved. Slide 25

Final Thoughts

*How **YOU** Doin'?*
NOW ?

Security & Privacy Roundtable: How YOU Doin'? Presented at HIPAACOW Fall 2004 Conference Copyright © 2004 Todd Fitzgerald/Lisa Gallagher All rights reserved. Slide 26



THANK YOU!

Contact Info:
Lisa Gallagher
Javelin Technology Group, LLC
Ellicott City, MD
lgallagher@comcast.net
(410) 531-2405

Todd Fitzgerald
United Government Services, LLC
Milwaukee, WI
Todd.Fitzgerald@cobalt-corp.com
Todd_Fitzgerald@yahoo.com
(414) 226-5812
www.UGSMedicare.com
www.Hipaacow.org

Security & Privacy Roundtable: How YOU Doin'? Presented at HIPAACOW Fall 2004 Conference Copyright © 2004 Todd Fitzgerald/Lisa Gallagher All rights reserved. Slide 27