WEDi SNIP Strategic National Implementation Process

HIPAA 101

Security Final Rule Standards

Susan A. Miller, JD

Sue Miller's HIPAA and Healthcare Information Services

Lesley Berkeyheiser, Principal

The Clayton Group

9th National HIPAA Summit

Getting Started

- The structure of the security rule relies on standards and implementation specifications in three major areas:
  - Administrative Safeguards;
  - Physical Safeguards; and
  - Technical Safeguards.

Getting Started

- There are also two administrative standards:
  - Organizational Requirements, and
  - Policies and Procedures
- The compliance date for the HIPAA Security Rule is April 20, 2005, and
  - April 20, 2006 for small health plans

All Standards are required

BUT:

- ***Implementation specifications*** **provide more detail and can be either required or addressable**

Addressable

- If an *implementation specification* is addressable, a covered entity may:
  - Implement, if reasonable and appropriate
  - Implement an equivalent measure, if reasonable and appropriate
  - Not implement
- All actions and decisions must be based on sound, documented reasoning

Addressable

- **ADDRESSABLE DOES NOT MEAN OPTIONAL**
- If CMS had intended these items to be optional, it would have marked them optional, not addressable
- All addressable items must be addressed
- All decisions about addressable items must be documented

Compare S&P

- Privacy is the "what"/ Security the "how"
- Examples
- Places to go
  - Start with the Chart
  - "For the Record"
  - NIST/ ISO
    - Security's inherent "flexibility" is its best feature and its toughest challenge

Administrative Standards

- Security Management - required
  - Risk Analysis – required
  - Risk management – required
  - Sanction policy – required
  - Information system activity review - required
- Assigned Responsibility -- required

Administrative Standards

- **Workforce Security** - **required**
  - Authorization and/or supervision – **addressable**
  - Termination procedures – **addressable**
  - Workforce clearance procedures – **addressable**

Administrative Standards

- **Information Access Management – required**
  - **Isolating Clearinghouse – required**
  - **Access authorization – addressable**
  - **Access establishment and modification – addressable**

Administrative Standards

- Security Awareness and Training – required
  - Security reminders – addressable
  - Protection from malicious software – addressable
  - Log-in monitoring – addressable
  - Password management – addressable

Administrative Standards

- Contingency Plan – required
  - Data backup plan – required
  - Disaster recovery plan -- required
  - Emergency mode operation plan – required
  - Testing and revision procedure – addressable
  - Applications and data critically analysis -- addressable

Administrative Standards

- Security Incident Procedures – required
  - Response and reporting – required
- Evaluation – required
- Business Associate Contracts and Oral Arrangement
  - Written contract or other arrangement – required

Physical Standards

- Facility Access Controls – required
  - Contingency operations – addressable
  - Facility security plan – addressable
  - Access control and validation procedures – addressable
  - Maintenance records – addressable

Physical Standards

- Workstation Use – required
- Workstation Security – required
- Device and Media Controls – required
  - Disposal – required
  - Media re-use – required
  - Accountability – addressable
  - Data backup and storage – addressable

Technical Standards

- **Access Controls** – required
  - Unique user identification – required
  - Emergency access procedure – required
  - Automatic logoff – addressable
  - Encryption and decryption – addressable

Technical Standards

- Audit Controls – required
- Integrity – required
  - Mechanism to authenticate ePHI – addressable
- Person or Entity Authentication – required
- Transmission Security – required
  - Integrity controls – addressable
  - Encryption – addressable

WEDi SNIP Strategic National Implementation Process

5 Steps to HIPAA Security Compliance

- *Read the Rule*
  - Determine what your organization needs for documentation, implementing new technology, upgrading old technology and documenting your decisions.
- *Perform a Risk Analysis*
  - A risk analysis forms the basis for your organization's ongoing risk management. You will identify your organization's deficiencies and establish a framework to develop appropriate security measures.
- *Select a security official*
  - This seems like a simple mandate, but the person designated must participate in the risk analysis and be involved in all the ongoing security management.

5 Steps to HIPAA Security Compliance cont

- *Identify the Strategy Your Organization Will Follow*
  - Upon completion of your organization’s risk assessment your organization will make determinations on how you will deal with your deficiencies now and in the future.
- *Develop or Update Policies and Procedures*
  - As part of your organization’s risk analysis include another column for evaluating your current policies and procedures. The gaps discovered with this review will fit into your plan to complete your HIPAA security work.

Tasks for HIPAA Security Compliance

- *Task #1*
  - Read the HIPAA Security Rule
- *Task #2*
  - Select a Security Analysis Tool
  - Compare Tool to HIPAA Security Rule
  - Review Financial and Audit Reports
  - Assemble Your Organization’s Team, and
  - Complete Your Organization’s Risk Assessment

Tasks for HIPAA Security Compliance

- *Task #3*
  - Draft security official Job Description, and
  - Name security official
- *Task #4*
  - Using Risk Assessment Identify Tasks/Risks to be Addressed, and
  - Establish a Plan for Tasks/Risks Identified, Including a Timeline

Tasks for HIPAA Security Compliance

- *Task #5*
  - Review, Update, and Document Changes in Existing Policies
  - Develop New Policies and Procedures
  - Add Policies as Necessary for Changes and Updates to Your Organization's Security Program
  - Train on Updated & New Policies and Procedures, and
  - Make Policies and Procedures Easily Accessible for Your Organization

Resources

- WEDI SNIP Security and Privacy White Papers and PowerPoint Presentations
- http://www.wedi.org/snip/public/articles/dis_publicDisplay.cfm?docType=6&wptype=2

Resources

- **Security and Privacy White Papers and PowerPoint Presentations**
- WEDI/SNIP White Paper disclaimer statement
- Security and Privacy Workgroup Introduction
- Privacy White Paper Overview, January 2004
- Security White Paper Overview, January 2004

Resources

- **White Papers Being Revised:**

  08/03/2004 SECURITY: Risk Analysis White Paper, Version 1.0, July 2004
  04/30/2004 SECURITY: Small Practice Implementation White Paper, Version 2.0, 04/28/2004
  02/11/2004 SECURITY: NIST/URAC/WEDI Healthcare Security Work Group White Paper, 2/11/2004
  02/02/2004 SECURITY: Audit Trail Clarification White Paper, Version 5.0, 11/07/2003

Resources

- White papers under development
  - Disaster Recovery
  - Employer II

WEDi SNIP Strategic National Implementation Process

Resources

- **White Papers Completed:**

08/10/2004 SECURITY: Evaluation, Final Version
08/10/2004 SECURITY: NIST SP 800 Series White Paper, Final Version
08/10/2004 SECURITY AND PRIVACY: Enforcement White Paper, Part I, Final Version
08/10/2004 SECURITY AND PRIVACY: Employer Issues White Paper, Part I, Final Version
08/10/2004 PRIVACY: Auditing Privacy Compliance, Final Version

Resources

- **White Papers Completed:**

  02/04/2004 SECURITY: Introduction to Security, Final Version
  02/03/2004 SECURITY: Introduction to Security Final Rule, Final Version
  02/02/2004 SECURITY: Security Policies and Procedures (P&P) White Paper, Final Version
  02/01/2004 SECURITY: Email and Encryption White Paper, Final Version
  01/31/2004 PRIVACY: Privacy Policies and Procedures White Paper, Final Version
  01/31/2004

Resources

- **White Papers Completed:**

  01/31/2004 PRIVACY: Small Practice Implementation White Paper, Final Version
  01/30/2004 PRIVACY: Access and Amendment White Paper, Final Version
  01/29/2004 PRIVACY: Accounting of Disclosures, Final Version
  01/28/2004 PRIVACY: De-identification White Paper, Final Version
  01/27/2004 PRIVACY: Minimum Necessary White Paper, Final Version

Resources

- **White Papers Completed:**

01/26/2004 PRIVACY: Notice and Authorization White Paper, Final Version
01/25/2004 PRIVACY: Oral Communications White Paper, Final Version
01/24/2004 PRIVACY: Paper Verses Electronic Records White Paper, Final Version
01/23/2004 PRIVACY: Preemption White Paper, Final Version
01/22/2004 SECURITY AND PRIVACY: Business Associate Example: Medical Transcription White Paper, Final Version
01/21/2004 SECURITY AND PRIVACY: Organizational Change Management White Paper, Final Version

Acknowledgements

- WEDI/SNIP would like to thank the following for preparing this presentation:
  - Lesley Berkeyheiser, The Clayton Group LBerkeyheiser@theclaytongroup.org
  - Sue Miller, J.D., Sue Miller’s HIPAA and Healthcare Information Service, tmsam@aol.com