



HCCA'S 12TH ANNUAL COMPLIANCE INSTITUTE

APRIL 13-16, 2008 | NEW ORLEANS, LA | HILTON RIVERSIDE NEW ORLEANS

IT'S OFFICIAL: GOVERNMENT AUDITING OF SECURITY RULE COMPLIANCE

Catherine Boerner, JD, CHC, President, Boerner Consulting, LLC
Nancy Davis, MS, RHIA, Director of Privacy/Security Officer, Ministry
Health Care



www.hcca-info.org | 888-580-8373



OBJECTIVES

- Provide a Brief Overview of the HIPAA Security Rule and Key Standards
- Describe the Oversight and Audit Process for Security Rule Compliance and Enforcement
- Review the Questions that the Government May Ask During an Audit
- Discuss Strategies and Tools Designed to Demonstrate Compliance



www.hcca-info.org | 888-580-8373

2

OVERVIEW OF HIPAA SECURITY RULE

- Final security standards for HIPAA were published on February 20, 2003. Under the Security Rule, health insurers, healthcare providers, and healthcare clearinghouses must establish procedures and mechanisms to protect the confidentiality, integrity and availability of electronic protected health information.
- The rule requires covered entities to implement administrative, physical, and technical safeguards to protect electronic protected health information that they receive, store, or transmit.
- Effective Date: April 21, 2005



www.hcca-info.org | 888-580-8373

3

SECURITY RULE STANDARDS

- Scalable - In determining how to apply the standards, covered entities should take into account their size, complexity, capabilities, costs of complying with the standards, and the potential risks to their electronic protected health information.
- Technology neutral - The standards do not specify any particular technology. They outline what must be done, not how to do it.
- Designed to protect electronic data at rest and in transit through administrative, physical, and technical safeguards



www.hcca-info.org | 888-580-8373

4

RELATIONSHIP TO PRIVACY RULE

- The Security Rule standards work in concert with the final Privacy Rule standards which were effective April 14, 2003. The two sets of standards use many of the same terms and definitions in order to make it easier for covered entities to comply.



www.hcca-info.org | 888-580-8373

5

OVERSIGHT AND ENFORCEMENT - CMS

- Enforcement Assigned to Centers for Medicare and Medicaid Services (CMS)
- CMS has authority to investigate complaints of non-compliance related to all of the HIPAA regulations other than the Privacy Rule. CMS' authority does not extend to enforcement of the HIPAA Privacy Rule; which is under the authority of the Office for Civil Rights (OCR). However, when privacy issues occur in the context of potential security violations, CMS and OCR collaborate to enforce the HIPAA rules.



www.hcca-info.org | 888-580-8373

6

CMS ANNOUNCEMENT – FEBRUARY, 2008

- In late February, CMS posts information on “HIPAA Onsite Compliance Reviews and Investigations.”
- CMS Office of E-Health Standards and Services (OESS) to utilize contracted services to assist with onsite investigations and onsite compliance reviews related to potential HIPAA Security Rule violations.
 - Onsite investigations may be triggered by complaints alleging non-compliance.
 - Onsite compliance reviews may arise from non-complaint related sources of information such as media reports or self-reported incidents.

NEW SLIDE



www.hcca-info.org | 888-580-8373

7

CMS INTERVIEW & DOCUMENT REQUEST

- With February announcement, CMS also posted:
 - Sample – Interview and Document Request for HIPAA Security Onsite Investigations and Compliance Reviews
 - “Not a comprehensive list of applicable investigation/review areas nor does it attempt to address all non-compliance scenarios. The individual circumstances of each applicable case will dictate the type of information that will be requested during an investigation or review.”

<http://www.cms.hhs.gov/Enforcement/Downloads/InformationRequestforComplianceReviews.pdf>

NEW SLIDE



www.hcca-info.org | 888-580-8373

8

INTERVIEW & DOCUMENT REQUEST - *Continued*

- Personnel That May Be Interviewed
- Documents and Other Information That May Be Requested for Interviews/Reviews:
 - Policies and Procedures and Other Evidence
 - Other Documents

NEW SLIDE



www.hcca-info.org | 888-580-8373

9

CMS & OCR – REPORTED SECURITY & PRIVACY RELATED COMPLAINTS

April 2005 – February 29, 2008

295 HIPAA Security Complaints Received

- 73 Open
- 222 Closed

April 2003 - February 29, 2008

33,916 HIPAA Privacy Complaints Received

- 6,961 Open
- 26,955 Closed

- OCR refers cases that describe a potential violation of the HIPAA Security Rule to the Centers for Medicare & Medicaid Services (CMS). OCR has made over 215 such referrals to CMS.

UPDATED SLIDE



www.hcca-info.org | 888-580-8373

10

CMS & OCR – REPORTED SECURITY & PRIVACY RELATED COMPLAINTS

February 29, 2008

Most Common Security Complaints

- Information Access Management
- Security Awareness and Training
- Access Control
- Workstation Use
- Security Incident Procedures

February 29, 2008

Most Common Privacy Complaints

- Impermissible Uses & Disclosures
- Lack of Safeguards
- Lack of patient access to their protected health information
- Uses or Disclosures of more than the minimum necessary
- Lack of or invalid authorization

UPDATED SLIDE



www.hcca-info.org | 888-580-8373

11

CMS CONTRACT - PRICEWATERHOUSECOOPERS

- CMS Announced Contract with PwC to Conduct Security Audits (Compliance Reviews) of Covered Entities
- Target: Covered Entities Which CMS has Already Received a Complaint
- To Evaluate Security Rule Compliance/Corrective Action Plans Following Complaint



www.hcca-info.org | 888-580-8373

12

OVERSIGHT AND ENFORCEMENT - OIG

- Department of Health & Human Services Office of Inspector General
 - OIG performs independent reviews of DHHS programs pursuant to the Inspector General Act of 1978 through the Office of Audit Services.
 - “Watchdog” agency responsible for reviewing CMS’ oversight, implementation, and enforcement of the HIPAA Security Rule.
 - Piedmont Hospital, Atlanta, Georgia (2007)
 - Cedars-Sinai Medical Center, Los Angeles, California (2008)



www.hcca-info.org | 888-580-8373

13

“REQUIRED” VS. ADDRESSABLE

- **REQUIRED**
 - Covered entities must implement.
- **ADDRESSABLE**
 - Covered entities must assess what is reasonable and appropriate for the organization (scalable)



www.hcca-info.org | 888-580-8373

14

KEY STANDARDS

- **Administrative**
 - Security Management Process
 - Assigned Security Responsibility
 - Workforce Security
 - Information Access Management
 - Security Awareness and Training
 - Security Incident Procedures
 - Contingency Plan
 - Evaluation
 - Business Associate Contracts and Other Arrangements



www.hcca-info.org | 888-580-8373

15

KEY STANDARDS - CONTINUED

- **Physical**
 - Facility Access Controls
 - Workstation Use
 - Workstation Security
 - Device and Media Controls
- **Technical**
 - Access Controls
 - Audit Controls
 - Integrity
 - Person or Entity Authentication
 - Transmission Security



www.hcca-info.org | 888-580-8373

16

COMPLIANCE CHALLENGES

1. Longstanding history of IT being “exempt” from external influences (regulations, standards, etc.).
2. IT staff may have sound knowledge of security practices and often have safeguards in place – but rarely have documentation to support practices (policies and procedures).
3. Generally, IT more comfortable in the technical world but less so in the compliance world.



www.hcca-info.org | 888-580-8373

17

COMPLIANCE STRATEGIES

- Perform a Comprehensive Risk Assessment
 - Security Rule Requirement
- Create Risk Assessment Action Plan and Follow Through
- Conduct Regular Assessments/Audits
- Establish Appropriate Policies and Procedures



www.hcca-info.org | 888-580-8373

18

RECOMMENDED SUPPORT DOCUMENTATION

- Policies & Procedures
 - Authentication Standards
 - Workstation Use & Security
 - Security Incident Response
 - Data Back-up
 - E-Mail Communications & Retention
 - Remote Access
 - Auditing of Access
 - Data Center Security
 - Portable Devices
- Other
 - Risk Analysis/Assessment
 - Educational Tools
 - Computer Access Agreements
 - Security Incident Form
 - Business Associate Agreement
 - IT Disaster/Contingency Plan



www.hcca-info.org | 888-580-8373

19

CURRENT OVERSIGHT ACTIVITIES

- Piedmont Hospital Experience – First Security Audit of a Private Entity (Spring, 2007)
 - Focused on Administrative, Physical and Technical Safeguards for ePHI
 - OIG On Site
 - Length of Audit Expected to be 10 Days – Lasted Several Months Due to Complexity (for both sides)



www.hcca-info.org | 888-580-8373

20

GENERAL PROBLEMATIC AREAS - AUDITS

- Lack of Documentation
- Missing or Incomplete Risk Analysis
- Lack of Effective Training for Workforce Members
- Ineffective, Incomplete, or Out-of-Date Policies and Procedures
- Inadequate Disaster Recovery and Business Continuity Plans
- Failure to Audit Use and Activity



www.hcca-info.org | 888-580-8373

21

HIPAA AUDIT: THE 42 QUESTIONS HHS MIGHT ASK

- “Unofficial” Copies of Piedmont Letter Circulating
 - Article by “Computer World”
 - <http://www.computerworld.com/action/article.do?command=printArticleBasic&articleId=9025253>
- Provider policies and procedures for ...
- 10 Day (Not Business Day) Turnaround



www.hcca-info.org | 888-580-8373

22

REVIEW OF 42 QUESTIONS

HANDOUT



www.hcca-info.org | 888-580-8373

23

COMPLIANCE TOOLS

- Risk Assessment – Initial and Ongoing
- Policies and Procedures
 - Up-to-Date
 - Communicated
 - Available
 - Enforced
- HIPAA Security Rule Matrix
- Security Rounds/Walk-Through (combine w/Privacy)



www.hcca-info.org | 888-580-8373

24

HIPAA SECURITY RULE MATRIX

- Develop Work Plan Based on Matrix
 - Standard/Section
 - Implementation Specifications
 - Required/Addressable
- Assigned Team or Person Responsible
- Implementation Solution
- Status



www.hcca-info.org | 888-580-8373

25

HANDOUTS

- OIG Audit Questions: Listing of “42 Requested Items” by the Office of Inspector General
- Sample Work Plan Summary Based on Security Rule Matrix – Ministry Health Care
- Sample Work Plan – Boerner Consulting, LLC
- Sample Assessment (Privacy & Security Rounds)



www.hcca-info.org | 888-580-8373

26

RESOURCES

CMS HIPAA Security Guidance at:

www.cms.hhs.gov/SecurityStandard/

- HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information

- HIPAA Security Educational Paper Series
 - Security 101 for Covered Entities
 - Security Standards Administrative Safeguards
 - Security Standards Physical Safeguards
 - Security Standards Technical Safeguards
 - Security Standards Organizational, Policies and Procedures and Documentation Requirements
 - Basic of Risk Analysis and Risk Management



www.hcca-info.org | 888-580-8373

27

RESOURCES - CONTINUED

- National Institute of Standards and Technology (NIST)
 - An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule***
 - NIST Special Publication 800-66, March 2005
 - <http://csrc.nist.gov/publications/nistpubs/800-66/SP800-66.pdf>

- HIPAA Collaborative of Wisconsin
 - www.hipaacow.org



www.hcca-info.org | 888-580-8373

28

CONTACT INFORMATION

- Catherine Boerner, JD, CHC, President, Boerner Consulting, LLC

cboerner@boernerconsultingllc.com

- Nancy Davis, MS, RHIA, Director of Privacy/Security Officer, Ministry Health Care

davisn@ministryhealth.org



www.hcca-info.org | 888-580-8373

29