The Law and The Reality

Grace Wiechman, CISSP
Guidant Corporation
grace.wiechman@guidant.com
Objectives

• Types of data to be secured
• What the HIPAA Security Rule requires
• The technical basis of the Rule
• Security in the unique setting of healthcare
Vocabulary

• **Covered Entity**
  • Healthcare providers (doctors, nurses ...), hospitals, insurance companies, self-funded employee benefit programs, insurance clearing houses

• **Protected Health Information (PHI)**
  • Info about a patient and their treatment that is identifiable

• **Business Associate**
  • Another business that provides a service to the covered entity (cleaning service, accountants, software and hardware vendors, etc.) where PHI may be disclosed
Patient Perspective

- Trust the healthcare provider and you to keep information private and secure
- Want timely and accurate access to their medical information for best care
- They’ve heard of HIPAA – but it’s just some paperwork they sign
- Patients may occasionally be attorneys or worse yet, security professionals
HIPAA In A Nutshell

HIPAA

Title I
Healthcare Portability

Title II
Fraud/Abuse & Administrative Simplification

Title III, IV, V (other)

Privacy
Transaction Standards and Code Sets
Employer Identifiers
Security Standards
Healthcare Provider Identifier

Future Standards

Effective 4/13/03 10/16/03 7/30/04 4/21/05 5/23/07
What Is PHI?

Protected Health Information (PHI) – 
Individually identifiable health information held or provided by Covered Entity includes the following or more:

- Name
- Address
- Dates
- Phone number
- Fax Number
- E-mail address
- Social Security Number
- Medical Record Number
- Health Plan Number
- Account Number
- Certificate/License Number
- Vehicle Identifier
- Device Identifier
- WEB URLs
- IP Address
- Biometric Identifier
- Full Face Photo
- Any Other Unique ID

There May Be More Than This List
What PHI Are We Most Likely To See?

- Patient Name
- Patient demographics
- Model numbers/Serial numbers
- Medical Record Numbers
- Social Security Numbers
- Date of Birth

Patient information becomes PHI when data about the patient is created or collected by a healthcare provider, insurance company or clearinghouse.
Is This Protected Health Information?

Your snoopy sister-in-law goes through your medicine cabinet while dining at your house and discovers you are on an antibiotic?

Your well meaning neighbor mentions your uncle has an appointment with Dr. Johnson when he calls with your appointment reminder?
Is This Protected Health Information?

No, if the patient is not identified

Yes, if the patient is identified
PHI Characteristics

- Lots of storage
  - Electronic patient records
  - Pervasive monitoring
- Ability to retrieve data off archives
  - 6 – 21+ years retention requirements
- Large increase of data as new data is added to electronic medical record
- Real-time or near real-time data
PHI Data Sizes in Treatment Settings

• **Radiology**
  - Average radiology exam: 50 MB/image
  - CT single multi-slice – 0.5 megabytes
  - Spinal Lumbar images – 10 MB
  - Spinal cervical images – 5 MB
  - Initial disk configuration: number of patients/year * number of exams * number of years required to store ~ 15 TB

Source:


http://www.himss.org 2002 conference
HIPAA Security Rule

Title I
Healthcare Portability

Title II
Fraud/Abuse & Administrative Simplification

Title III, IV, V (other)

Privacy

Transaction Standards and Code Sets

Employer Identifiers

Security Standards

Healthcare Provider Identifier

Future Standards

Effective 4/13/03 10/16/03 7/30/04 4/21/05 5/23/07

Administrative Safeguards

Physical Safeguards

Technical Safeguards
Electronic PHI

• Security Rule applies only to electronic PHI
• Privacy Rule covers electronic, paper and oral PHI
• Document image storage is moving paper into the electronic realm
HIPAA Security Key Ideas

1. Ongoing Risk Analysis/Risk Management
2. Administrative Safeguards
3. Technical Safeguards
4. Physical safeguards
5. “Required” and “Addressable”

- Enforcement starts April 21, 2005
- Privacy rule has security requirement
• **Required** – must implement

• **Addressable**
  • If reasonable and appropriate – must implement
  • If not feasible:
    • Alternative security measure
    • Combination of both
    • Not implement

• **Considerations**
  • Risk factors, risk mitigation already in place
  • Cost
  • **Size of organization**
  • **Document rationale!**
Administrative Safeguards

- **Security Management Process**
  - Risk Analysis (R)
  - Risk Management (R)
  - Sanction Policy (R)
  - Information System Activity Review (R)

- **Assigned Security Responsibility (R)**

- **Workforce Security**
  - Authorization and supervision (A)
  - Workforce clearance procedure (A)
  - Termination procedures (A)
Administrative Safeguards - continued

- **Information Access Management**
  - Access authorization (A)
  - Access establishment and modification (A)

- **Security Awareness and Training**
  - Security reminders (A)
  - Log-in monitoring (A)
  - Password management (A)

- **Security Incident Procedures**
  - Response and reporting (R)
• Contingency plan
  • Data backup plan (R)
  • Disaster recovery plan (R)
  • Emergency mode operation plan (R)
  • Testing and Revision Procedure (A)
  • Applications and Data Criticality Analysis (A)

• Evaluation (R)

• Business Associate Contracts and Other Arrangements
  • Written Contract or Other Arrangements (R)
Physical Safeguards

• Facility Access Controls
  • Contingency Operations (A)
  • Facility Security Plan (A)
  • Access Control and Validation Procedures (A)
  • Maintenance Records (A)

• Workstation Use (R)

• Device and Media Controls
  • Disposal (R)
  • Media Re-use (R)
  • Accountability (A)
  • Data Backup and Storage (A)
Technical Safeguards

- Access Control
  - Unique User Identification (R)
  - Emergency Access Procedure (R)
  - Automatic Logoff (A)
  - Encryption and Decryption (A)
- Audit Controls (R)
Technical Safeguards Continued

• Integrity
  • Mechanism to Authenticate Electronic PHI (A)
• Person or Entity Authentication (R)
• Transmission Security
  • Integrity Controls (A)
  • Encryption (A)
Things of Note About the Law

• Not a specification of algorithms or techniques
• No specific software required
• Flexible but hard to do
• Technical controls and people controls
• Constant re-evaluation
• More administrative than technical controls
Why Is This A Big Deal?

• First criminal conviction under the HIPAA Privacy Rule August 19, 2004


• Identity Theft

• Not clear if civil and criminal penalties apply only to covered entity
HIPAA Security Rule References – Mapped Standards circa 1998

- ANSI X3.92 Data Encryption Standard
- ANSI X9 Public key and encryption
- ASTM – Standards for healthcare security
- FDA electronic signatures final rule
- FIPS publications 112, 196, 46-2
- IEEE 802.10, 802.10c
- IETF 1422, 1424, 1423
- ISO/IEC 9798, 10164-4, 10164-5, 10164-7, 10164-8
- NIST – Generally Accepted Principles and Practices for Secure Systems
- RFC 1510 Kerberos
HIPAA Security Rule References

- **NIST**
  - NIST Computer Security Division 893 and CSRC Home Page

- **HHS**
  - Administrative Simplification
  - Office for Civil Rights - Privacy of Health Records
    - [http://www.hhs.gov/ocr/hipaa/](http://www.hhs.gov/ocr/hipaa/)

- **Other**
  - HIPAA regs - Searchable HIPAA regulations
    - [http://www.hipaadvisory.com/regs/](http://www.hipaadvisory.com/regs/)
Healthcare Security Realities

- No way to uniquely identify a patient everywhere
- Patients may have multiple healthcare providers
- Stupid interactions with the HIPAA privacy rule
- Health care providers may not be able to complete a computer transaction in a given time
- Staff may work in multiple areas of a hospital or clinic
- Physicians often practice at multiple clinics or hospitals
- Budgets are tight, new patient treatment equipment gets funding
- Hundreds of disparate systems
Data Confidentiality (Encryption)

- Data “Hiding”. This is the typical function when people think of Cryptography.
- Can be as simple as an alphabet substitution algorithm such as “rot13”:
  
  A B C D E F G H I J K L M
  N O P Q R S T U V W X Y Z

  Message:
The quick brown fox jumps over the lazy dog.

  Rotated 13 characters and sent:
  Gur dhvpx oebja sbk whzcf bire gur ynml qbt.

  Recipient rotates 13 characters again:
The quick brown fox jumps over the lazy dog.

Note: This is an example of a very simple symmetric algorithm where the same method for “encrypting” is used for “decrypting”

Data Integrity (“Message Digest”)

- Create a small and unique “digest” from the message. Also called a checksum, hash or message digest.
- Computationally infeasible to produce two different messages having the same Message Digest.
- Even the smallest change in the message will result in a completely different message digest.
- Aids in verifying what was sent matches what was received.

  Common methods are MD5 and SHA-1

  Message:
The quick brown fox jumps over the lazy dog.

  MD5 Digest:
  0d7006cd055e94cf614587e1d2ae0c8e

  SHA-1 Digest:
  9c04cd6372077e9b11f70ca111c9807dc7137e4b

Proof of Authenticity (Digital Signature)

- Combine a message digest with asymmetric encryption to offer data integrity and an assurance that the source holds the signing credentials.
- Does not provide data hiding.

  The quick brown fox jumps over the lazy dog.

  The quick brown fox jumps over the lazy dog.

  ---Begin Signature---
  MIICtQYJKoZIhvcNAQcCoIICpjCCAgICAQExCzA JBgUrDgMCgUAMASGCSqGSIb3…
  --- End Signature---
Confusing Points in HIPAA Security

- Returning or destroying data?
- Determining what is a reportable security incident?
  - Firewall log attempt?
  - Virus or worm?
  - Internal improper use of data?
  - Equipment loss or theft?
  - Decommissioning equipment?

Not always clear when these are required or how to do them
How Do You Balance?

- Responsible protection of PHI and accessibility?
- Overwhelming your customer with too much information?
- Defining what types of incidents should be communicated?
- Tradeoffs between acceptable business risk and security?
Equipment Decommissioning

What do we do with media containing PHI?

- Medical equipment
- Disk drives
- Floppy drives
- CD disks

Devices getting smaller

New devices to store PHI in ways not imagined
Options For Disposal

- Erase, remove, destroy PHI on the media

Most Data is Recoverable

- Most simple erasure methods leave data recoverable
- Media destruction is often the only cost-effective solution
PHI Destruction

• **Physical destruction**
  - Shredding vendors
  - De-gaussing

• **Issues**
  - How does this work with a RAID disk?
  - How can you be certain your disposal vendors are not reselling the parts?
Security Recommendations

- Security built into systems from concept onward
- Easy to understand actions for the non-technical user
- System designs that are correctly configured upon delivery
- Think about security from and end-to-end perspective
- Consider digital signing of critical structures
Security Recommendations

- Protect data in transit and at rest
- Disposal issues for software and hardware
- Work with industry groups to promote best practice and good standards
Final Thoughts

People and processes, algorithms and software are the keys to good security.
What Questions Do You Have?
HIPAA

Grace Wiechman, CISSP
grace.wiechman@guidant.com
Guidant Corporation