HIPAA and CPR Architecture

Baptist Health Systems of SF
Overview

• Main risks in CPR related to security
• HIPAA and its role in CPR risks
  – Brief overview
  – Related [proposed] regulations
• Projects related to CPR security
• What CORBA security covers in HIPAA-related security requirements and what it does not
All Requirements from One Goal

- to earn as much money as possible and
- to lose as little money as possible
- “security” has never brought any money to a healthcare organization
- a security infrastructure can either cause or prevent loss of money
Main Risks: Loss of Money

- Lawsuits because of mal-treatment
  - Occasionally, < $10M

- Loss of customers
  - Loss of accreditation
    - Up to 50% of revenues
  - Customers prefer more “secure” providers
    - Maybe in the future, < 10-20% of revenues
Main Risks: Loss of Money (2)

- Financial penalties
  - < $100K/year
- Classaction lawsuits because of federal or state legislation breaches
  - Rarely, ≅ $100M
HIPAA main parts
as it pertains to healthcare organizations

Subtitle F, Sec. 262
Goal: improving the operation of the health care system and reducing administrative costs

HIPAA
Ammends
Social Security Act

Title II
Subtitle F, Sec. 262

Title XI
Part C: Administrative Simplification

section 1173
DHHS Secretary
To adopt and review

Secretary of Commerce
To coordinate

Standards

Safeguards
Health Care Provider clearing house plan

Ensure the integrity and confidentiality of the information

To maintain

To ensure the integrity and confidentiality of the information

To protect the information

To protect the information

To ensure compliance with this part by the officers and employees

Any reasonably anticipated threats or hazards to the security or integrity of the information

Any reasonably anticipated unauthorized uses or disclosures of the information

Unique Health Identifier
Security for Health Information
Transactions and transactions data
Code Sets
Electronic Signatures

Ensure the integrity and confidentiality of the information

Ensure compliance with this part by the officers and employees

Specify procedures

Against any reasonably anticipated threats or hazards to the security or integrity of the information

With respect to:
- Individual,
- Employer,
- Health plan,
- Health care provider

To specify

Transfer of Information

Electronic transmission and authentication of signatures

Health claims or equivalent encounter information
Health claims attachments.
Enrollment and disenrollment in a health plan.
Eligibility for a health plan.
Health care payment and remittance advice.
Health plan premium payments.
First report of injury.
Health claim status.
Referral certification and authorization.

To coordinate

To adopt and review

To adopt and review

To adopt and review
HIPAA Milestones

Proposed Rules from DHHS:
- National Standard Health Care Provider Identifier
- Standards for Electronic Transactions and Code Sets

Security and Electronic Signature Standards
Proposed Rules from DHHS

Today


HIPAA becomes federal law

Recommendations from DHHS
secretary with respect to the privacy of individually identifiable health information is due

Legislation with respect to the privacy of individually identifiable health information is due

Final regulations from DHHS secretary with respect to the privacy of individually identifiable health information is due if the congress defaults for 8/99 due date.

Standards Legislated by the Congress or by DHHS

large healthcare providers, clearing houses and plans to comply with the standards

Copyright © 1999 Baptist Health Systems of SF
HIPAA: Security Requirements

Potential Risks

Vulnerabilities

Individual Health Data in Electronic Form

Require

To Assess

Appropriate Security Measures

Develop

Implement

Maintain

Document

Keep Current
HIPAA: Security Requirements

Administrative Procedures
- Certification
- Chain of Trust
- Partner Agreement
- Formal Mechanism for Processing Records
- Personnel Security
- Security Management Process
- Training
- Internal Audit

Physical Safeguards
- Assigned Security Responsibility
- Media Controls
- Physical Access Controls
- Policy Guideline on Workstation use
- Secure Workstation Location
- Security Awareness Training

Technical Security Mechanisms
- Integrity Controls
- Message Authentication
- Access Controls
- Encryption
- Event Reporting
- Abnormal Conditions Alarms
- Audit Trail
- Entity Authentication

If using networks
- Audit Trail
- Entity Authentication

Technical Security Services
- Access Control
- Audit Controls
- Authorization Control
- Data Authentication
- Entity Authentication

Policy Guideline on Workstation use
- Secure Workstation Location
- Termination Procedures
- Security Incident Procedures
- Contingency Plan

Security Management Process
- Security Configuration Management
- Security Incident Procedures
- Contingency Plan

Internal Audit
- Chain of Trust
- Partner Agreement
- Formal Mechanism for Processing Records
- Physical Access Controls
- Security Configuration Management
- Security Incident Procedures
- Contingency Plan

April 19, 1999

Copyright © 1999 Baptist Health Systems of SF
HIPAA: Communication Security Requirements

- Technical Security Mechanisms (communication security)
  - Integrity Controls
  - Message Authentication
  - Access Controls or Encryption
  - Audit Trail
  - Event Reporting
  - Abnormal Conditions Alarms
  - Entity Authentication

If Using Networks
HIPAA: Technical Security Services Requirements

- **CORBA Technical Security Services**
  - **Access Control**
    - Procedure for Emergency Access
    - Optional Encryption
    - Context-based AC
    - RBAC
  - **Authorization Control**
    - At least one
    - Either one
  - **Audit Controls**
    - Automatic Log off
  - **Data Authentication**
    - At least one
    - Biometrics
    - Telephone Callback
  - **Entity Authentication**
    - Unique User Identifier
    - Password
    - Token
    - PIN
CPR Architecture Goals

• Based on CORBA technology
  – Use CORBA Security, HRAC/RAD

• Integrated with existing systems
  – Integration via CA’s Unicenter/TNG
  – Integration with firewall infrastructure
  – Integration with directory infrastructure

• Integration with upcoming technologies
  – PKI
  – Smart card and biometric authentication
Current Projects towards CPR security

- SSO with Unicenter/TNG for existing systems
- New firewall
- Computerized Patient Record (CPR) security policies WG
- NDS redesign
- Standard authorization service for application-level access control
- CORBA-security services
Future Projects towards CPR security

- PKI
- Smart cards
- Biometric authentication
- VPN
Security of CORBA Technical Services

- CORBA Security + RAD
  - Procedure for Emergency Access
  - Optional Encryption
  - At least one
  - Either one
  - Context-based AC
  - RBAC
  - User-based AC

- CORBA Security
  - Automatic Log off
  - Entity Authentication
  - Unique User Identifier
  - At least one
    - Biometric
    - Telephone Callback
    - Password
    - Token
    - PIN
  - Smart card-based Authentication

- CORBA Security + RAD
  - Access Control
  - Authorization Control
  - Audit Controls
  - Data Authentication

April 19, 1999

Copyright © 1999 Baptist Health Systems of SF
CORBA-based CPR: Communication Security

- Integrity Controls
- Message Authentication
- Access Controls
- Encryption
- Audit Trail
- Event Reporting
- Abnormal Conditions Alarms
- Entity Authentication

If Using Networks
FYI: CORBA and RAD