Security Requirements in Healthcare

Konstantin Beznosov
beznosov@baptisthealth.net

Baptist Health Systems of SF

OMG doc # corbamed/99-03-16
Introduction

- OMG -- forum for software vendors
- What about users?
  - to let them know about distributed technology we need
  - wanted technologies are standardized
- This presentation objective
  - What US healthcare wants from security vendors
Overview

• Risks

• Requirements
  – Security requirements to the healthcare organizations
  – functional and non-functional requirements for security architectures

• BHSSSF example to illustrate
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
- Class lawsuits because of federal or state legislation breaches
  - Rarely, ≈ $100M
HIPAA: Security Requirements

Require

To Assess

Potential Risks
Vulnerabilities

Individual Health Data in Electronic Form

Appropriate Security Measures

Develop

Implement

Maintain

Document

Keep Current

for protection of
HIPAA: Security Requirements

- Administrative Procedures
  - Certification
  - Formal Mechanism for Processing Records
  - Personnel Security
  - Security Management Process
  - Training
  - Internal Audit

- Physical Safeguards
  - Assigned Security Responsibility
  - Physical Access Controls
  - Secure Workstation Location
  - Security Awareness Training

- Technical Security Mechanisms
  - Integrity Controls
  - Access Controls
  - Event Reporting
  - Audit Trail

- Technical Security Services
  - Message Authentication
  - Encryption
  - Abnormal Conditions Alarms
  - Entity Authentication

- If using networks
  - Authorization Control
  - Data Authentication

- Policy Guidance on Workstation use
  - Security Configuration Management
  - Termination Procedures
  - Security Incident Procedures

- Media Controls
  - Physical Access Controls
  - Policy Guideline on Workstation use

- Chain of Trust
  - Partner Agreement

- Access Control
  - Audit Controls

- Audit Trail
  - Entity Authentication

- Security Incident Procedures
  - Contingency Plan

March 23, 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

If Using Networks

- Audit Trail
- Event Reporting
- Abnormal Conditions
- Alarms
- Entity Authentication
HIPAA: Technical Security Services Requirements

Technical Security Services

- Access Control
  - Procedure for Emergency Access
  - Optional Encryption
- Authorization Control
  - Context-based AC
  - RBAC
- Audit Controls
  - Automatic Log off
  - At least one
- Data Authentication
  - Either one
  - Entity Authentication
    - At least one
    - Unique User Identifier
    - Optional Encryption
      - Biometric
      - Telephone Callback
      - Password
      - Token
      - PIN
- Authorization Control
  - User-based AC
  - At least one
  - Either one
- Authorization Control
  - RBAC
  - User-based AC
BHS Example: Background

- 5 different hospitals and clinics covering most of South Florida residents
- y2k inventory listed about 150 applications
  - probably 50 are pure clinical
- Centralized IT department
- Average IT professional
  - does not have formal CS degree
  - around 5 years of experience in healthcare IT
BHS Example: existing systems

- Clinical systems are from all major vendors
- Separate user name and password for each system
- Developed NDS infrastructure used for file, printer, groupware services
- Firewall, NT-based dial-up
- Deploying CA’s Unicenter/TNG for legacy integration; will work with NDS
BHS Example: New Systems

- All CORBA-based
- Use HRAC/RAD for authorization
- Integrated with exiting systems
BHS Example: Security-related Projects

- Computerized Patient Record (CPR) security policies WG -- to produce consistent set of security policies
- Consolidation of user security attributes in NDS, and deployment of LDAP gateways
- PKI & smart card plans
- Deployment of CORBA-security services
BHS Example: Functional Requirements for Security

- Enable compliance with HIPAA-related requirements on security and digital signatures
- Enable compliance with state legislation
- Help to pass inspections from state and federal accreditation commissions
- Provide unified (access control, QoP) policy languages.
BHS Example: Nonfunctional Requirements for Security

- Integrate with CORBA technology
- Use LDAP-compliant directory service for storing user security attributes and public keys (at least)
- Integrate with access control mechanisms of legacy systems via CA’s Unicenter/TNG
- Provide maintenance and administration tools useful for average IT professionals
- Be known, reliable and dependable vendor