

HIPAA SECURITY

NEW YORK STATE SOCIETY OF CERTIFIED PUBLIC ACCOUNTANTS
EMERGING TECHNOLOGIES TECHNICAL SESSION

Joel Lanz, Principal
JOEL LANZ, CPA, P.C.
WWW.SYSTEMSCPA.COM
JLANZ@ITRISKMGMT.COM

AGENDA

- Introduction & Overview
- Security Rule Overview
 - Administrative Procedures
 - Physical Safeguards
 - Technical Security Services
 - Technical Security Mechanisms
- To-Dos and Related Challenges
- Security Risk Assessment Methodologies for Small and Mid-Size Organizations
- Conclusion

INTRODUCTION AND OVERVIEW

JOEL'S PARADIGM

- Over 20 years of IT risk management experience ranging from one-person “IT shops” to global organizations
- Practicing CPA with prior experience as a Big 5 Technology Risk Partner and an Internal Audit Vice President
- Adjunct faculty member at Pace University's Graduate School of Computer Science and Information Systems
- Professional Certifications
 - Certified Information Systems Security Professional (CISSP)
 - Certified Information Systems Auditor (CISA)
 - AICPA's Certified Information Technology Professional (CITP)
- Publications, etc., etc.

WHAT IS SECURITY?

- PER THE AMERICAN HERITAGE COLLEGE DICTIONARY

- Freedom from risk or danger
- Freedom from doubt, anxiety or fear
- Something that gives or assures safety
- Something deposited or given as assurance of the fulfillment of an obligation

- PER HIPAA

- The regulations which address the protection of data resident on provider computers or networks, as well as the protection of data while it is being transmitted to third parties
- Primarily the technical components that address the collection, protection, and dissemination of data

WHY ARE ORGANIZATIONS SECURITY-CHALLENGED?

- Abdication of responsibilities
- Inability to segregate activities
- Calculator mentality
- Putting out fires
- Information overload
- Expectation gap
- Inadequate training
- Ignorance and false pride

WHAT'S THE GOAL?

- To Determine the Organization's Security Gap Within the Five Areas of Compliance:
 - Administrative Procedures
 - Physical Safeguards
 - Technical Security Services
 - Technical Security Mechanisms
 - Electronic Signature Standards (???????)

TONIGHT'S OBJECTIVE



ADMINISTRATIVE PROCEDURES

ADMINISTRATIVE PROCEDURES

- Certification of Systems and Networks
 - Goal is to verify that appropriate security is in place
 - Use of outside consultants for large organizations, internal resources for small organizations
 - Standard is evolving

ADMINISTRATIVE PROCEDURES (CONT.)

- CHAIN OF TRUST PARTNER AGREEMENT
 - Goal is to protect data exchanged between third parties
 - Responsibility and liability for business partner actions
 - Requires significant lead time to identify business partners and draft/negotiate agreements

ADMINISTRATIVE PROCEDURES (CONT.)

- CONTINGENCY PLAN FOR SYSTEM EMERGENCIES
 - Need for backups, alternate processing options, disaster recovery procedures
 - Need for applications and data criticality analysis

ADMINISTRATIVE PROCEDURES (CONT.)

- FORMAL MECHANISM FOR PROCESSING RECORDS
 - Policy/procedure for receipt, manipulation, storage, dissemination, transmission and disposal of health information
- INFORMATION ACCESS CONTROL
 - Policy/procedure for granting different levels of access to health information

ADMINISTRATIVE PROCEDURES (CONT.)

- PERSONNEL SECURITY
 - Need to show adequate supervision of system maintenance personnel
 - Need to show maintenance of access authorization records
 - Clearance procedures for personnel
 - Training for users on security

ADMINISTRATIVE PROCEDURES (CONT.)

- SECURITY CONFIGURATION MANAGEMENT

- Demonstrate that security is part of standard hardware/software configuration management
- Need documentation, testing, scanners, virus checking

- INTERNAL AUDIT

- Ongoing regular audit process for log-ins, file access, security, incidents, etc.

ADMINISTRATIVE PROCEDURES (CONT.)

- SECURITY INCIDENT PROCEDURES
 - Documented instructions for reporting and responding to security breaches
 - Enforcement
- SECURITY MANAGEMENT PROCESS
 - Policy/procedures for risk analysis, risk management, sanctions and security
 - Goal is to prevent, detect, contain and correct security breaches

ADMINISTRATIVE PROCEDURES (CONT.)

- TRAINING

- Applicable to all staff
- Security is part of everyone's job
- Must include awareness training, periodic reminders, specific user education on security threats and personal computer protection and use

- TERMINATION PROCEDURES

- Formal instructions for ending access
- Policies on changing locks, removal from access lists, removal of system accounts and returning access devices

PHYSICAL SAFEGUARDS

PHYSICAL SAFEGUARDS (CONT.)

- ASSIGNED SECURITY RESPONSIBILITY
 - Either specific individual or specific organization/department
- MEDIA CONTROLS
 - Policy/procedure for receipt and removal of hardware and software in and out of the organization

PHYSICAL SAFEGUARDS (CONT.)

- PHYSICAL ACCESS CONTROLS
 - Policy/procedure which covers disaster recovery, equipment control, facility security, sign-in procedures, and need to-know-definitions
- POLICY/GUIDELINE ON WORKSTATION USE
 - Governs proper use of workstations, including time-outs

PHYSICAL SAFEGUARDS (CONT.)

- **SECURE WORKSTATION LOCATION**
 - Goal is to eliminate or minimize unauthorized access to health information
 - Evaluate physical locations, access and display
- **SECURITY AWARENESS TRAINING**
 - Applies to all staff, agents, contractors
 - Make security part of the daily activities

TECHNICAL SECURITY SERVICES

TECHNICAL SECURITY SERVICES (CONT.)

- ACCESS CONTROLS

- Limit access to health information to those employees with business need
- Based upon context, role or user
- Encryption optional

- AUDIT CONTROLS

- Mechanisms to record and examine system activity

TECHNICAL SECURITY SERVICES (CONT.)

- **AUTHORIZATION CONTROL**

- Mechanism to obtain consent to use and disclose health information through implementation of role or user based access

- **DATA AUTHENTICICATION**

- Verification that data has not been altered or destroyed
- Implementation includes check digits, double keying, digital signature

TECHNICAL SECURITY SERVICES (CONT.)

- ENTITY AUTHENTICATION

- Process to prove that entity is who they claim to be
- Implementation to include biometric id systems, passwords, PINs, telephone callback, security tokens
- May have different standards for on and off campus access

TECHNICAL SECURITY MECHANISMS AND ELECTRONIC SIGNATURE STANDARDS

TECHNICAL SECURITY MECHANISMS

- Guard against unauthorized data access over a communications network
- Need for encryption on open networks like the internet and dial-in lines
- Need alarm, audit trail, entity authentication, event reporting

ELECTRONIC SIGNATURE STANDARDS

- Cryptographically based digital signature is the standard for HIPAA transactions
- Electronic signature is not required (???)
Sometimes required) for currently proposed HIPAA transactions

TO-DO's AND RELATED CHALLENGES

TO-DO's AND RELATED CHALLENGES –

Awareness and Education

■ TO-DO's

- Train project team on HIPAA data security guidelines
- Identify and train key system users
- Conduct meetings with primary system vendors

■ CHALLENGES

- HIPAA is “good practices”
- IT is already on board and awaiting budget
- Level of compliances dependent upon vendors and use of vendor features

TO-DO's AND RELATED CHALLENGES –

Policy & Procedure Review

■ TO-DO's

- Identify relevant policies and procedures
- Analyze against HIPAA guidelines
- Identify gaps and missing policies and procedures

■ CHALLENGES

- Inconsistent policies and procedures for same system
- Systems within organization don't have consistent policies & procedures
- Policies for new technologies don't exist

TO-DO's AND RELATED CHALLENGES – System Review

■ TO-DO's

- Inventory systems, databases, interfaces that contain patient information
- Collect current contact information for vendors
- Evaluate each system against guidelines

■ CHALLENGES

- System and vendor information is hard to get and maintain
- Usually requires more than one person to do
- Security features are available but not used

TO-DO's AND RELATED CHALLENGES –

Other Documentation Review

■ TO-DO's

- Review disaster recovery plan, medical staff by-laws, IT job description
- Determine what is missing or not current

■ CHALLENGES

- Disaster recovery more relevant in these times and to senior management
- Medical staff more cooperative regarding security
- Role of security officer will be “baked in” to strategies

TO-DO's AND RELATED CHALLENGES – Staff Interviews

■ TO-DO's

- Identify gaps between policies & porcedures and current practices
- View security in action
- Assess general staff awareness of security

■ CHALLENGES

- The software “ease-of-use” challenge creates security exposures
- Hardware is vulnerable too
- Security not traditionally a major IT training initiative

TO-DO's AND RELATED CHALLENGES – Contract Review

■ TO-DO's

- Determine potential cost of HIPAA upgrades
- Identify vendor's obligations regarding patient data security

■ CHALLENGES

- Effectiveness of regulatory conformance clause
- Application of chain-of-trust concept
- Outsourcers need detailed consideration

TO-DO's AND RELATED CHALLENGES – Technical Review

■ TO-DO's

- Assess security of infrastructure and connections outside
- Inventory security tools and determine effectiveness

■ CHALLENGES

- Technical people usually know what is needed, although they may need to be assisted with cost/risk analysis
- Lack of funding
- No security system is perfect

TO-DO's AND RELATED CHALLENGES – GAP Identification

■ TO-DO's

- Identify gaps in current environment against HIPAA guidelines
- Consider alternate scenarios for mitigating the risk and complying

■ CHALLENGES

- Multiple strategies for achieving compliance exist – what's most cost-effective?
- It may not be possible to completely close all gaps in the required timeframe

TO-DO's AND RELATED CHALLENGES – Compliance Plan

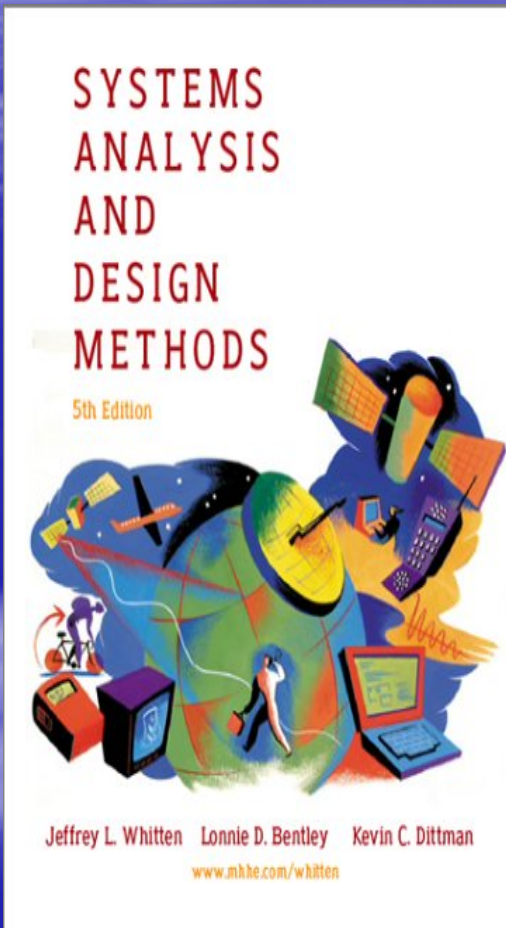
■ TO-DO's

- Define recommendations
- Identify priority, timing, resources, cost and risk
- Build a work plan

■ CHALLENGES

- Some overlap with other HIPAA work teams
- Some project work may be delayed
- Temporary resources (e.g., consultants) may be required)

WHERE'S THE RISK?



HOW MUCH TO FIX?

- Not as much as you would expect
- You don't necessarily need to purchase advanced technology
- 80% of the problems can be resolved very cost-effectively
- Organizational culture and behavior modification require the greater efforts



SECURITY CONCLUSION

A team sport that doesn't necessarily require the most fancy equipment to win - but does require you to understand the fundamentals of the game and that you and your team must provide best efforts to win!

Otherwise –

you are playing to just give the ball to the other side.

CONTACT INFORMATION

Joel Lanz

Principal

Joel Lanz, CPA, P.C.

P.O. Box 597

Jericho, NY 11753-0597

(516) 637-7288

www.systemscpa.com

jlanz@itriskmgt.com