

HIMSS
INTRODUCTION TO HEALTHCARE INFORMATION
AND MANAGEMENT SYSTEMS-
WHERE CONCEPTS CONVERGE

PATIENT CONFIDENTIALITY
AND SECURITY ISSUES

Deborah Kohn, MPH, RRA, FHIMSS

Principal

Dak Systems Consulting

650.345.9900

dkohn@daksystemsconsulting.com

DISCLAIMER

NOTICE OF LIABILITY

- **Dak Systems Consulting has made every effort to make this presentation as accurate as possible. However, names, firms, web sites, etc., change constantly. In addition, there may be inadvertent mistakes of content and typography. Consequently, the author makes no guarantees, warranties or representations of any kind.**
- **Inclusion or exclusion in this presentation of any vendor, product, organization or service does not constitute an endorsement or a rejection by Dak Systems Consulting.**

PURPOSE

- **With increasing mobilization toward electronic patient records and current federal legislative events, patient confidentiality and health information security issues are critical to healthcare organization risk management.**

OBJECTIVES

- **Define commonly used terms**
- **Identify healthcare organizational security**
 - common threats
 - infrastructure components
 - models
 - sample strategies/policies
 - sample educational programs
 - responsibilities
- **HIPAA readiness**
- **Assess the risks!**

DEFINITIONS

CONFIDENTIALITY

Confidentiality is a status
indicating that information is
s e n s i t i v e .

CONFIDENTIALITY

- It is a universally accepted notion that the information in patient and employee medical, financial, and administrative records is **confidential**.

CONFIDENTIALITY PATIENT RECORDS

- Information in **patient records** is **confidential** because it is held that:
 - the relationship between the patient and the provider of care is special
 - the communication between the patient and the provider of care should be protected from disclosure

CONFIDENTIALITY PATIENT RECORDS

- **This concept is supported in the physicians' code of ethics and in the law.**

PROVIDER-PATIENT RELATIONSHIP PRIVILEGE

- The **provider-patient relationship** is considered a **patient privilege**.

PROVIDER-PATIENT RELATIONSHIP PRIVILEGE

- A **privilege** is a statutorily created prohibition which prevents a provider who attended a patient from testifying in a court or similar proceeding about the diagnosis, care, or treatment that the provider rendered to the patient
 - unless the patient consents to such testimony, or, by the patient's conduct, waives the protection.

PROVIDER-PATIENT RELATIONSHIP PRIVILEGE

- The **provider-patient privilege** is justified legally and ethically because society believes that patients ought to be secure in disclosing information to their healthcare providers so that providers will be able to treat the patient fully.

PROTECTING THE PRIVILEGE

- Unless the patient waives the protection, access to confidential information must be controlled:
 - to protect the confidential information
 - to protect the privacy of the individual

PROTECTING THE PRIVILEGE

- For example, patient records, **regardless of on what medium they are stored**, may be removed from a healthcare organization's jurisdiction and safekeeping only in accordance with a court order, subpoena, or statute.

PROTECTING THE PRIVILEGE

- The protection varies considerably by state.
- The protection is more strictly applied to cases of mental illness, substance abuse, and HIV.

WAIVING THE PROTECTION: RELEASING THE INFORMATION WRITTEN AUTHORIZATION

- By waiving the protection, a patient or his/her legal representative must provide **written authorization to release the information**, unless otherwise required by law.

EXCEPTIONS

Patient records, regardless of on what medium they are stored, may be examined by:

- **persons against whom actions have been brought for personal injuries**
- **the healthcare organization to:**
 - **provide better patient care**
 - **measure the effectiveness of its medical staff**
 - **undertake educational programs**
 - **undertake research**
 - **protect itself from suit.**

Patient records, regardless of on what medium they are stored, may be examined by:

- **employees of providers to:**
 - **perform their legitimate, provider-related duties**
- **external consultants retained by the provider and/or patient**
 - **insurance companies**
 - **legal counsel**
 - **law enforcement officials**
 - **photocopy services**
 - **auditors**

SECURITY

The protection of confidential patient information and the protection of individual privacy place **special responsibilities** on the healthcare organizations that are held accountable for the information systems that process and store the patient information.

SECURITY

- Information **security** assures confidentiality.
 - It protects confidential information from accidental or intentional disclosure to unauthorized persons.
 - It protects confidential information from error, loss, or destruction.
 - It protects confidential information from unauthorized alteration or tampering.

COMMON THREATS

■ Theft

- Desktop, laptop, palmtop computers and the data/information they contain are especially vulnerable to theft from inside or outside the organization

■ Hackers

- Persons who gain illegal entrance into a computer system
- Serious problem!

COMMON THREATS

■ Sabotage

- Insiders constitute the greatest threat to data/information security!

■ Malicious Code

- Viruses
- Trojan Horses
- Logic Bombs
 - May be harmless pranks, such as displaying unwanted phrases or graphics
 - May be serious - destroying data, crashing systems, changing data, holding data hostage

COMMON THREATS

■ Disgruntled Employees

- Insiders constitute the greatest threat to data/information security!
- Why passwords must be deleted immediately when an employee resigns or is discharged

■ Physical Problems

- Power Failures (outages, spikes, brownouts)
- Fires/Floods/Strikes

COMMON THREATS

■ Errors and Omissions

- Unintentional by legitimate users

■ Browsing

- Legitimate users attempting to access information they do not need to know, just to satisfy their curiosity

SECURITY MEASURES

- Therefore, any information system that processes and stores confidential patient information **MUST** incorporate information **security measures.**

SECURITY MEASURES

- Operational
- System
- Data/Information

SECURITY MEASURES

OPERATIONAL

- **Includes the processes and procedures by which the confidentiality of all information collected, stored, retrieved and transmitted is ensured.**

SECURITY MEASURES SYSTEM

- **Includes the methods and techniques that ensure the confidentiality of information within analog and digital information systems.**

SECURITY MEASURES

DATA/ INFORMATION

- **The sum total of all technical mechanisms and procedures employed to ensure that data/information are entered, accessed and changed only in an authorized and prescribed manner.**

SECURITY MEASURES

All Are Interdependent

and

All Must Be Packaged Together!

MODEL PACKET OF SECURITY MEASURES

- **Define the institutional requirements for confidentiality and security**
- **Describe the safeguards that will be utilized**
- **Establish strict penalties for noncompliance to the safeguards**
- **Provide a means to enact the penalties**
- **Outline confidentiality and security education programs for system administration and users**
- **Specify contractual requirements for systems and technology vendors/suppliers**

MODEL SAFEGUARDS

OPERATIONAL

- **Confidentiality standards and ramifications for violating these standards**
- **A standard policy describing data user responsibility for confidentiality**
- **Confidentiality agreements with all authorized users, including outside computer vendors**
- **Policies for patient access, including guidelines for information requests**

MODEL SAFEGUARDS SYSTEM

- **24 hour a day user support**
- **Strict policies prohibiting sharing of access codes**
- **Vendor contractual obligations which identify specific protections and when they will be initiated**

MODEL SAFEGUARDS SYSTEM (continued)

- **Documented maintenance requirements, procedures, and logs**
- **Documented system downtime instructions for users and technicians**
- **Documented backup and recovery procedures**

MODEL SAFEGUARDS

DATA/INFORMATION

- **Physical controls over access to the system inputs and outputs, such as unique passwords, identification numbers, fingerprints, voiceprint, locks, badges**
- **System controls for access tracking, such as audit trails, automatic monitoring of computer transactions, and automatic logoffs**
- **Operational controls for access, such as defining authorized users and data access on a need-to-know basis**

SUCCESSFUL SECURITY STRATEGY

- **Initiate a close working relationship with HIM professionals who have experience dealing with the legal and ethical issues of health information**
- **Identify existing weaknesses in security, authentication mechanisms, and administrative procedures for existing systems, databases and electronic repositories**

SUCCESSFUL SECURITY STRATEGY

- **Implement a program to improve security awareness for all users, and reevaluate existing policies for all employees**
- **Include business partners in the plan, especially payors and IS vendors, to assure that all health information received from the organization is handled with the appropriate safeguards**

ORGANIZATION-WIDE SECURITY POLICY SCOPE

■ Does It???

- Apply to ALL INFORMATION owned by or in custody of the organization, regardless of its form or storage medium
- Have support from the highest level of your organization
- Define confidentiality obligations of ALL outside agencies receiving patient information access
- Apply across all information types

ORGANIZATION-WIDE SECURITY POLICY

LEGAL/REGULATORY REQUIREMENTS

■ Does It Incorporate???

- Federal Regulations**
- State Laws**
- Licensing Agencies**
- JCAHO / NCQA/ HIPAA Requirements**
- Professional Ethics**

ORGANIZATION-WIDE SECURITY POLICY DISTRIBUTION

- **To Whom Are the Security Policies Made Available?**
- **Are Security Policy Acknowledgments Required?**
- **Are Periodic Renewals Required?**
- **What Processes Are in Place to Ensure that the Public Has Access to the Security Policies?**

ORGANIZATION-WIDE SECURITY POLICY CONTENT

- Does It Include???
- Organizational Philosophy
- Organizational Accountability
- Patient, Provider, Public Rights
- Classification of Information
- Access
- Records of Access

ORGANIZATION-WIDE SECURITY POLICY CONTENT (continued)

- **Does It Include???**
 - **Collection, Retention and Destruction Issues**
 - **Awareness Training**
 - **Monitoring and Auditing**
 - **Maintenance**
 - **Disaster Recovery**

ORGANIZATION-WIDE SECURITY POLICY ISSUES

- **Access Controls (System Log-Ons, Audit Trails)**
- **Access to Information (Levels of Access, Access to Other Employees' Files)**
- **Access to Information by Patients and Their Family Members**
- **Access to Information by Physicians and Their Office Staff**

ORGANIZATION-WIDE SECURITY POLICY ISSUES

- **Access to Information for Research**
- **Acquisition of Software**
- **Acquisition of Hardware**
- **Anti-viral Software Use**
- **Back-up Procedures**
- **Bringing in Diskettes/Downloading
Information From Outside the Organization**

ORGANIZATION-WIDE SECURITY POLICY ISSUES

- **Dictation and Transcription of Patient Reports**
- **Disaster Recovery**
- **Disposal of Printed Reports**
- **Electronic Data Interchange Use**
- **Electronic Mail Use**
- **Elevator / Hallway Discussion**
- **Encryption of Files**

ORGANIZATION-WIDE SECURITY POLICY ISSUES

- **Home Use of Organization Hardware/Software**
- **Internet Access**
- **Malicious Code**
- **Passwords and Other, Related Access
Control Measures**
- **Penalties for Violation**
- **Privacy Rights (Patient, Employees,
Providers)**

ORGANIZATION-WIDE SECURITY POLICY ISSUES

- **Protection of Proprietary Information**
- **Remote Access to Information Systems
(Manual or Digital)**
- **Retention, Archiving, and Destruction of
Information, Regardless of Storage Medium**
- **Security Breaches**
- **Staff Responsibility for Data Accuracy and
Integrity**

ORGANIZATION-WIDE SECURITY POLICY ISSUES

- **Staff Responsibility for Data Confidentiality**
- **Use and Monitoring of Security Alarms**
- **Unauthorized Software**
- **Vendor Access to Information Systems**

SECURITY EDUCATION PLAN

■ Basic Education Program

- Presented to Employees with Limited Access to Patient Information
- Content:
 - Security Video
 - Confidentiality Agreement
 - Confidentiality and Security Overview

SECURITY EDUCATION PLAN

- **Intermediate Education Program**
 - **Presented to Employees with High Access to Patient Information**
 - **Content:**
 - **Basic Education Program**
 - **Faxing / Email Protocols**
 - **V / Email Etiquette**
 - **Liability Issues for Self and Organization**
 - **Audit Processes**
 - **Disposal of Paper**
 - **Password Security**
 - **Electronic Signature**
 - **Virus Detection**

SECURITY EDUCATION PLAN

■ Management Education Program

- Presented to Collaborative Management Team, Department Heads, and Administration
- Content:
 - Basic and Intermediate Education Programs
 - Management Role Accountabilities
 - Granting Access Levels
 - Identifying High-Risk Situations
 - Performing a Risk Assessment
 - Staff Accountability
 - Role Modeling
 - Unit/Department-based Data Management, Manipulation and Distribution Issues
 - Implementing New Technologies

RESPONSIBILITIES

- **Because even the most stringent information security measures designed and implemented can go wrong ...**

RESPONSIBILITIES

... the **commitment** for information security in terms of policies, procedures, and financial support must come from the executive level of healthcare management.

RESPONSIBILITIES

... the **task** to secure information in terms of information system capabilities must come from the information system designers.

RESPONSIBILITIES

... the **task** to maintain and enforce the procedures, computing environments, communications networks, etc., under which security prevails must come from Health Information Managers (HIMs), Chief Security Officers (CSOs), or similarly-designated professionals.

RESPONSIBILITIES

**Technology Will Meet the
Challenge and Provide Solutions**

**We Have an Obligation to
Recognize the Benefits of
Technology and Apply Them!**

HIPAA READINESS

HIPAA

- **Standardization of Code Sets**
- **Healthcare Identifiers**
- **Claims Transactions**
- **Electronic Signature**
- **INFORMATION SECURITY**

HIPAA

INFORMATION SECURITY

- **Review the proposed standards and assess your organization's level of compliance by performing a risk analysis**
- **Become familiar with the information security standards and standards development organizations**
- **Identify existing organizational structures to aid development and implementation of an information security program**

HIPAA

INFORMATION SECURITY

- **Ensure that policies exist to control access to and release of patient-identifiable health information**
- **Ensure that users of electronic health information have unique access codes**
- **Ensure that each user's access is restricted to the information needed to do his/her job**

HIPAA

INFORMATION SECURITY

- **Outline provider responsibilities for protecting the confidentiality of health information in the staff bylaws or rules and regulations**
- **Outline employee responsibilities for protecting the confidentiality of health information in the employee handbook**
- **Train everyone with access to health information about confidentiality and their responsibilities regarding confidentiality**

HIPAA

INFORMATION SECURITY

- **Review vendor contracts for outsourcing of health information to ensure that they include provisions regarding confidentiality and information security**
- **Ensure that system managers, network managers, and programmers do not have unlimited and unrecorded access to patient information**

HIPAA

INFORMATION SECURITY

- **Monitor access to information and put corrective action plans in place for violation of organization policy**
- **Perform risk assessments to prioritize and continually improve the security of the systems**
- **Maintain current knowledge of information security issues and industry response to these issues**

ASSESS THE RISKS!