Implementation of Need to Know Policies Through Authorization Security Controls

John Travis, Director - Product Management, Cerner
Bob Robke, Director of Operations, Michiana Health
Maggie Goldberg, Security Consultant, Michiana Health
Presentation Outline

- Background on Cerner and MHIN
- Privacy and Security Complement
- Basic Elements of a Role Based Authorization Model
- Key Matters for Policy and Procedure Development
- MHIN’s Policy Objectives
- MHIN’s Implementation Experience
- MHIN’s Lessons Learned and Future Course
Cerner Corporation

- Founded in 1979
- Headquartered in Kansas City, MO
- Leading Provider of HCIS Across Continuum of Care
- More Than 1000 Provider Organizations Automated
- US and International Markets
- Seeking Common Denominator(s) for Privacy and Security Requirements (!)
MHIN Organization Model and Operating Structure

- Information Utility / Application Service Provider
- Indiana Limited Liability Company
  - Owners
    - Physician Directed Regional Reference Laboratory
    - Regional Integrated Delivery System
  - Participants
    - Hospitals
    - Laboratories
    - Physician Practices
    - Radiology Groups, Imaging Centers
    - Clinics
MHIN Organization Model and Operating Structure

- Community Model
  - Independent of Specific Entities
  - Complete Patient Record
  - Suppliers of Data - Hospitals, Laboratories, Ancillary Service Providers, Clinics / Physician Practices
  - Users of Data - Physicians, nurses, etc.

- Subscription Based Pricing
  - Data Suppliers (hospitals, labs) Provide Results to Data Users (physicians, practices)
  - Minimal upfront capital
MHIN Data and Services Model

**Hospitals**
- Surgery Reports
- Lab Results & Reports
- Radiology Reports
- Discharge Summaries
- Admission & Registrations
- Emergency Dept. Records
- Etc.

**South Bend Medical Foundation**
- Lab Results
- Pathology Reports

**Other Area Service Providers**
- Radiology groups
- Radiation Therapy
- Laboratories
- Ambulatory Surgery Centers

**Clinical Data Repository**

**Orders**

**Results**

**MHIN Services**

**Physician Network**
- Primary Care Physicians
- Clinic Physicians
- Cardiologists
- Orthopedic Surgeons
- Other Specialty Groups

**Orders**

**Results**
Privacy And Security – “Hand In Glove…..Sort Of”

• Originally Intended To Be Implemented Together
  – Can One Have Privacy Without Security?
  – Does Privacy Implementation Become Procedural and Security Implementation Technical?
  – Can Minimum Necessary Be Supported Absent Need To Know Policy

• One Take Away
  – Retain The Spirit of Security To Implement The Letter of Privacy
Security As Complement to Privacy

• Privacy (The Right)
  – Right of the individual to have anonymity
    • Confidence they will not be subjected to unwarranted intrusion

• Confidentiality (The Expectation)
  – Obligation of the custodian or user of an individual’s information to respect and uphold an individual’s privacy

• Security (The Mechanism)
  – Policies, procedures, mechanisms, tools, technologies and accountability methods to support Privacy
Minimum Necessary

• Procedural Definition
  – Using The Right Amount For The Purpose At Hand
  – Policy and Procedurally Based
  – Consider How To Justify Use of What Is Appropriate
  – Common Sense Dictate Of Care Provider Discretion
  – Feeds Into Need To Know Under Security Rule
Minimum Necessary

• Interesting Exception
  – Not Applicable To Disclosures Made for A Treatment Purpose
    • I Am Not Sure Why That Is In There BUT
      – Suggests Greater Care Taken For How Information Is Used Within The Entity
      – Less Control Over What Happens To Information Disclosed By An Entity
      – Highlights Importance Of Good Security Controls (more later)
Key Matters of Procedural Development

• Minimum Necessary Policies
  – Privacy Practices
    • Leads to Notice of Privacy
  – Drives Need to Know Definition
    • For Whatever Security Mechanisms You Develop, This Is A Must

• Need To Know Policies
  – Justify Based On Role and Responsibility
  – System of Record AND Information Access Rights
Planning Considerations

• For Implementation Planning
  – Define Common Sense Approaches That Balance Policy and Technology Roles In Support of Operations
  • Find The Common Denominator For Implementing Policy In Systems
    – Example
      » Role Based Need to Know vs User Based Need to Know
      » Does The Application Support Your Need To Know Policy As It Is? Are There Controls Absent?
      » Are There Things Policy Alone Should Solve?
  • Balance Availability Needs With Privacy Needs
    – You Need The Information To Provide Care But
      » Patient Has A Right To Understand How You Use and Disclose It
Security Components

- **Authentication**
  - You are who you say you are

- **Authorization**
  - You can see and do what you are permitted by policy to see and do

- **Accountability**
  - You are held responsible for what you do with what you see and for what you do
Authorization Models

- **Role Based**
  - Your Work Responsibility Defines Your Authorization Right

- **User Based**
  - Your Identify as An Individual Defines Your Authorization Right

- **Context Based**
  - A Combination of Who You Are, Where You Are, What You Are and When You Are What You Are Defines Your Authorization Right
## Examples of Authorization Security Elements

<table>
<thead>
<tr>
<th>Mechanism</th>
<th>Purpose</th>
<th>Role</th>
<th>Context</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Group</td>
<td>Access to applications</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Relationship</td>
<td>Access to Patient</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Organization</td>
<td>Access to Patients at a Facility</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Location</td>
<td>Access to a Place of Service</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Schedule</td>
<td>Present or Absent</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Privilege</td>
<td>Rights to Perform Operations on Patient Data</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Rights to Access Sensitive Info</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

xx: Confidentiality
xxx: Location
xx: Organization
x: Relationship
x: Schedule
x: Application
x: Group
x: Mechanism
MHIN’S Objectives

- Build the Community Based Complete Patient Record
  - Improve Patient Care
  - Improve Physicians’ Access to Information About Their Patients
  - Reduce / Eliminate Duplicate Tests and Costs
- Share Expensive Resources Among Providers Throughout the Community
  - Technology
  - People
  - Knowledge
- Reflect Community Standards
  - “Small Town” Environment
  - Cooperative Spirit
  - Concern for Invasions of Privacy
Toward The Complete Patient Record - Entity Focused Patient Charts

- Located Throughout the Community
- Contain Internal Information Only
- No Complete View of Patient’s Clinical Information
- Duplication / Missing Information Inevitable

Minimal Support for Physician and Patient
Building the Complete Patient Record

- Physician's Practice
- Patient's Complete Record
  - Reports B
    - Reference Laboratories
  - Reports C
    - Radiology / Imaging Services
  - Patient Chart A
  - Patient Chart B
  - Patient Chart C
  - Patient Chart D
  - Patient Chart E
  - Patient Chart F
- East Side Hospital
- West Side Hospital
- Ambulatory Surgery Center
MHIN’S Objectives and Information Sharing Implications

- Community Based Complete Patient Record - Multi-Entity CDR
  - Independently Owned and Managed Entities
  - Competitors

- Share Expensive Resources Among Providers
  - Sophisticated Technology Set-Up
  - Employees Playing Multiple Roles; Clearly Delineated Responsibilities Needed

- Reflect Community Standards - Small Town Environment
  - Negative Impact of Unauthorized Disclosure - One Mistake Can Sink the Ship
  - Understand and Incorporate Multiple Overlapping Relationships
    - Physicians, especially specialists, practice at multiple hospitals
    - Primary care dominated by IDN employed physician networks, though perceived by community as independent practices
    - Employees work in multiple locations and sometimes multiple positions
Information Sharing / Need to Know and MHIN’s Security Principles

- Community Standards Developed Beginning in 1995
- “Lock Down, then Open Up Depending on Specific Need” -- Not the Other Way Around!
- Security Principles (Examples):
  - Physicians and care givers provide care as members of organizations; they become system users by virtue of this same association with specific organization(s), e.g., hospital medical staff, nurse or physician in a specific medical practice.
  - Patients receive care through a relationship with a system user who is associated with a specific organization; access to a patient’s EMR is granted only when the user has a relationship with the organization where the encounter occurs and with the specific patient.
  - The information generated during an encounter at a specific organization belongs to that organization.
  - The policies of the organization determine the kind of access an employee or physician can have to the patient’s EMR.
Security Controls for Authorization

- Role Based Access Governed by Legitimate Relationship with the Patient
  - Automatic via Interfaces - Priority When Possible
  - Manual, if needed, for physicians only
- Physician Roles
  - Automatic: Admitting, Attending, Ordering, etc.
  - Manual: Anesthesiologist, Radiologist, etc.
- Employee Roles
  - Hospital Staff: Medical Service & Patient’s Location
  - Physician Practice Staff: Via a Specific Relationship Between the Staff Member and a Physician
Developing Access Guidelines and Security Controls

- Policy Objectives, Underlying Principles, and System Implications Relatively Clear

- Critical Issues Included
  - Whether a Role Will Typically be Established Automatically Via Interface or Not
  - Access for
    - Physicians
    - Hospital / Institutional Provider Staff
    - Physician Practice Staff
  - Access Among Entities of An Owned / Managed IDN
“Early Adopter” IDN - Prototype for Access Guidelines and Security Controls

- Many Similarities Between IDN and Community Model
  - “Owned and Managed” Doesn’t Mean Universal Access
  - Physician Networks - Objectives, Perceptions Among Physicians, Administrators, and Community may differ
- Scenarios and System Flows Developed
  - Specific Examples Requiring Access Guidelines, e.g.,
    - PCP Employed by IDN vs Independent PCP
    - Labs Drawn in Hospital vs Physician Office
    - Physician Practice Staff Access to Practice Data vs Hospital Data
  - Scenarios Included Detailed Process Map, e.g.,:
    - Encounter Process, Charting, Systems Flow
    - Physicians Who Are Part of the Encounter
    - Paper & Electronic Record “Owners & Keepers”
    - CDR Access - Location, Users, Types of Data
- Requirements Derived from Scenarios & Systems Flows
“Early Adopter” IDN - Prototype for Access Guidelines and Security Controls

- Dialogue with Physicians - Balance “Need to Know” with Physician Perspective
  - What the Physician Thinks S/He Should Be Able to See
  - What the Physician Wants Another Physician to See
- Access Guidelines - Physician Steering Committee
- Topics
  - Appropriate Roles, e.g., Admitting, Research
  - Need to Know - Physicians, Administrators, and Hospital Staff
  - Length of Time for Access, Re-Establishing Access
  - Access for Hospital Staff
- Process
  - Subcommittee met for approximately 6 weeks;
  - Recommendations to Physician Steering Committee
  - Incorporated in MHIN Policies and Procedures
- Monitoring and Remediation - Physician Input
Collaboration with Cerner

- Early Recognition of Need for Additional Functionality
  - IDN Model
  - Community Model
- Collaboration on Requirements For A Community Model
  - Task of Managing Access Not Just Within But Across Organizations
- Ongoing Work with Cerner Security Team
  - Scenarios
  - Requirements Definition
  - Alpha Site
  - Testing - New Functionality and Performance
Current Initiatives

- Functionality
  - Entity Based Security
    - A cornerstone of MHIN’s Security and Access
    - Relationship based override provided by Cerner
      - Importance of Managing Access Across Organizations In Context of Need to Know
  - Differentiating Longitudinal Access From Open Access
    - Longitudinal – Persistent Right For Long Term Access
    - Open – “Break the Glass” for Emergency Situations
  - Manage Both By Position
  - Goal: A Person’s Control of His / Her Record
Needs To Also Be Addressed

- Considering Access Needs In Community Beyond Clinicians
  - Non-Clinician Access Such As For Billers
    - Drive Based On Relationship to the Clinician
    - Managed Access Across Organizations
    - Access Right Conveyed To The User – Not Self Determined

- Managing Occasional or Unpredictable Access Needs
  - Third Party or Internal Auditors
  - Peer Reviewers
  - Quality Assurance
  - Consulting Clinicians
Current Initiatives - HIPAA

- Reviewing, Revising and Implementing Policy
- Monitoring Privacy Rule
  - Authorization Controls
  - Consent Issues
  - Audit Requirements
- Compliance Committees
  - MHIN Affiliates - hospitals, labs, etc.
  - MHIN Compliance
- Community HIPAA Task Force on Electronic Transfer of Information
- Ongoing Community Dialogue
Questions Anyone?