

# Health Information Exchange Privacy & Security

Alabama HIMSS Conference  
October 1-2, 2009

# Privacy/Security Issues for HIE

- Data Exchange Agreement
- Data Repository by HIE Partner (Minimum Necessary)
- Access Control
- Partner Data Retention
- Data Breach/Data Loss
- Patient Consent
- Partner compliance measurements

# Background for the Examples

- Kentucky and Ohio each have statutorily required Prescription Monitoring Programs (PMP)
- State law requires the submission of Schedule II-V prescriptions to the states for monitoring purposes
- A relatively new movement in the PMP world is to share data across states

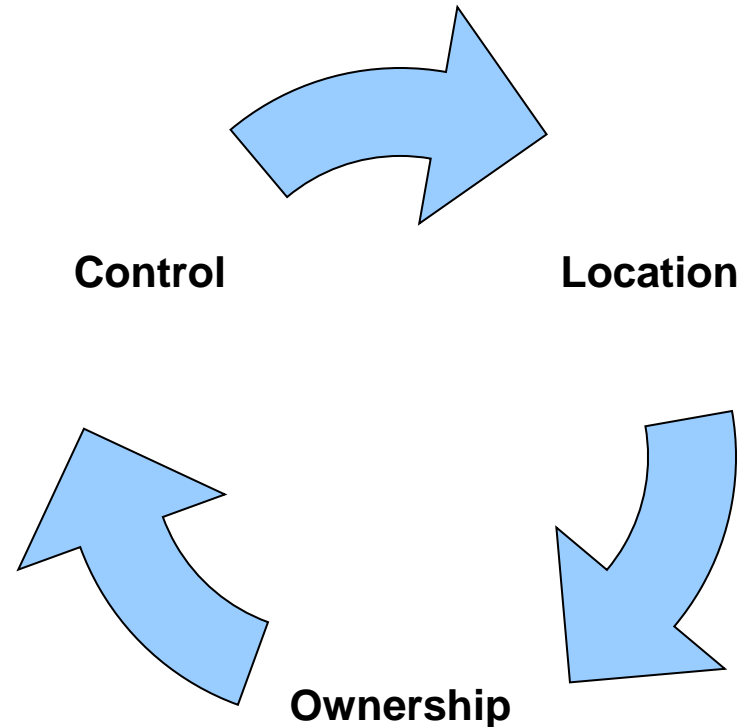
# Same Pieces But Different Puzzle

- The principles and regulatory guidance is still the same
- The manner in which they fit together is different



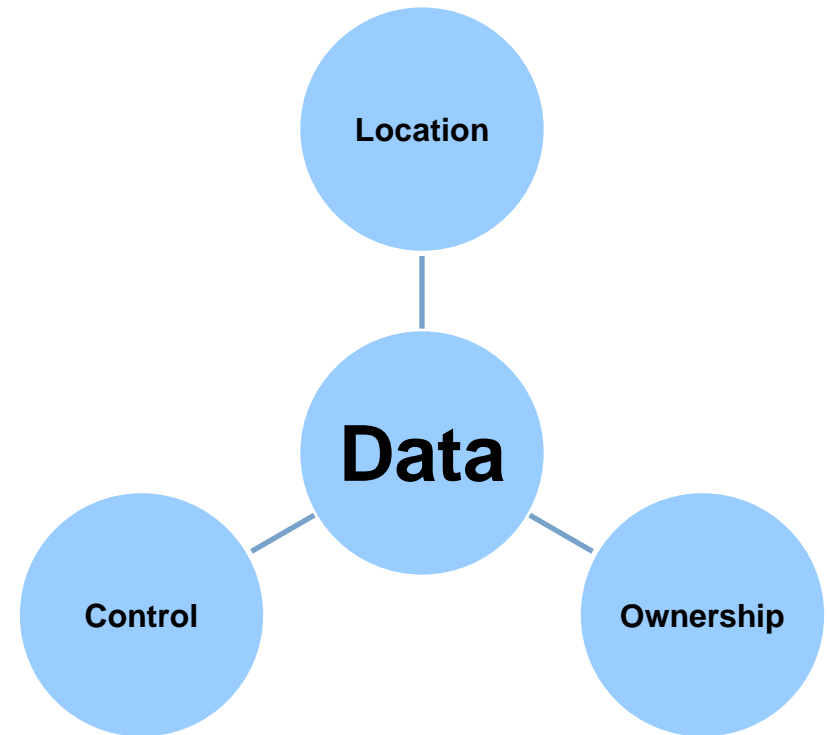
# Traditional Information Control is Centralized

- Traditional client/server or web-based information system creates a single control point for data

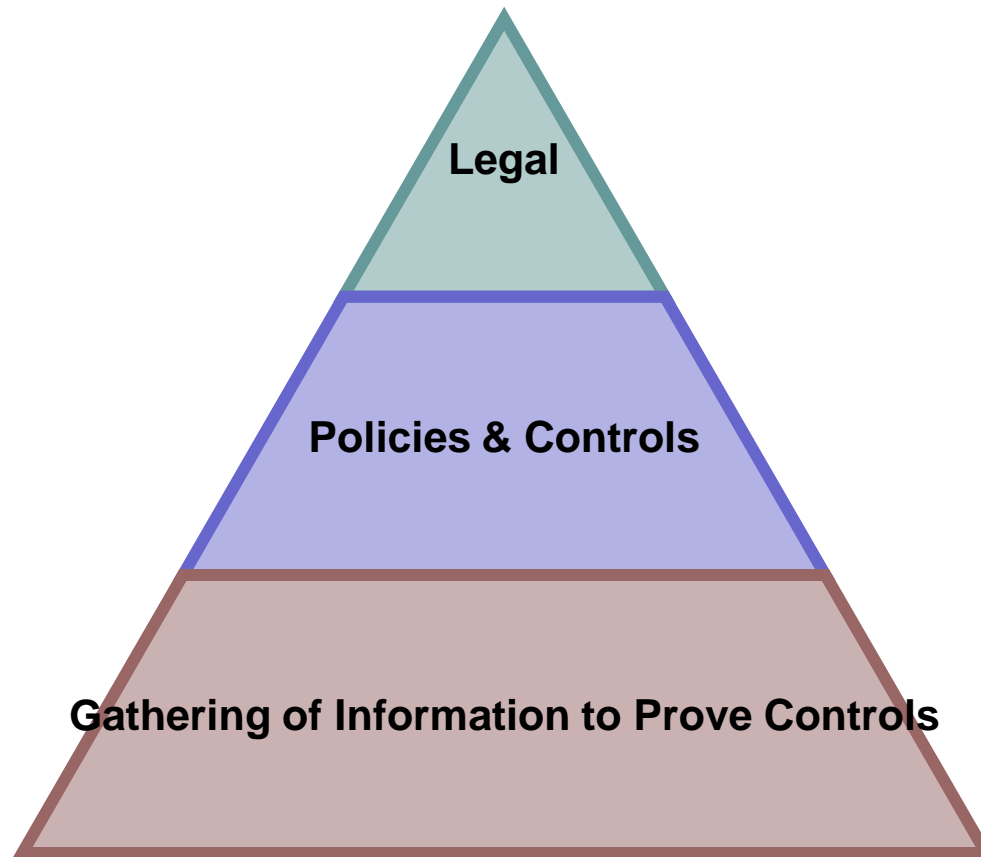


# HIE Information Control Dispersed

- The Health Information Exchange splits the core tenants on which we depend for privacy and security efficiency
- More players, more deciders, more lawyers



# Security Compliance Foundations



# Building the Framework

- Understanding that control is not centralized
- Increased importance of agreements to manage information inventory that leaves the organization
- Difficulty of balancing limited liability with the need for business to move forward

# Reducing Contradictory Legal Requirements

- National grants seeking to harmonize state law
- Even the most knowledgeable states are struggling with the details of implementing harmonized legal requirements
- In this example of two PMP programs sharing data, it involves 2 state laws, HIPAA, 1 state data breach notification law

# Compare & Rank Method

- Kentucky

- 8 authorized categories
- Peace officer includes “bona fide” investigation requirement

- Ohio

- 5 categories of authorized users
- Specifically permits an own user to get his or her own records
- Provide mechanism for an individual to get an outline to whom records have been provided

# Compare & Rank

## ● Kentucky

- Board of Licensure
- Board of Nursing
- Disciplinary Board
- ***Doc/Pharmacist***
- Peace Officer
- Medicaid
- Grand Jury
- Judge

## ● Ohio

- Licensure Board
- Peace Officer
- Grand Jury
- ***Doc/Pharmacist***
- Own Individual

# Create Measurements Whenever Possible

Category	High Cost	Risk %	Total Risk
Criminal Penalties	N/A	N/A	N/A
Data Breach/Data Loss	\$69 million	25%	\$17.25 million
Loss of Federal Funding	\$5 million	25%	\$1.25 million
Litigation	\$40 million	1%	\$400K
HIPAA Civil Penalties	\$1.5 million	1%	\$15K

# Sometimes You Have to Agree to Disagree

- Kentucky

- Treats as a Clearinghouse
- Must follow Security Rule
- BAA required

- Ohio

- Does not consider itself to be a covered entity
- Security Rule compliance not required
- No BAA required

# Be Practical

- Understand that it is not reasonable for all data uses to have explicit authorization
- Identify top-ranked risks
- Address top risks through contract first and then technical solutions

# The Final Product for the Data Exchange Agreement

- Ultimately limited access to only physicians and pharmacists
- Changed PMIX to be pass-through rather than data repository
- Added specific requirements for user authorization process
- Specified data retention period
- Required notification of business partner in data breach but did not specify liability

# Retention of Data by the HIE Partner

- Ohio state law requires no data to be kept longer than 2 years
- Kentucky rolls data to archive after 3 years
- Ohio report images kept for 30 days
- Kentucky report images kept for 2 years

## Minimum Necessary in the Control of Information

- KEY in HIE is transfer of information at the exact moment while needed but then the reclamation once need passes (difficult in provider setting)
- Longer retention increases risk
- Do the business uses match?

# Access Control

- How to identify users and their access?
- Sometimes you have to go with less access
- Difficulty of that for providers is that they rely on other staff to retrieve information
- Here--each party agreed to certify users with certain license or database matches

# Access Control with HIE Partner

- How do we identify users?
- Will they follow the same standards as our organization?
- How do we know if users still work at the Partner?
- Future of Access Control is monitoring behavior rather than monitoring stagnant user controls

# Data Breach Notification

- Ohio considers itself bound by Ohio data breach notification law
- During the process, Kentucky became bound by changes to HIPAA federal law concerning data breach notification
- Concerns were for legal pre-emption and, more importantly, which party is responsible for notice and costs in the event of a data breach

# Data Breach/Data Loss

- Agree to notify each other within 5 days of a data loss
- Remained silent on the issue of liability other than the general indemnification clause
- There have to be reasonable expectations since all scenarios can't be addressed

# Data Broker Tool Setup

- This was a pure technical security issue
- Debates were between a pass-through or a shared repository
- Pass-through prevailed at some cost of a better user experience
- Patient-oriented HIE may have to be a hybrid as more physicians build an EMR

# Partner Compliance Measurements

- Will be the method to manage security and privacy compliance in the future
- Self-certification is not enough
- Build trust of community through ongoing and regular measurements against standards

# Patient Consent

- Opt in or Opt out?
- If opt out—does the patient data have to be fully erased or can it remain in a master patient index and be hidden?
- The idea that patients can manage their own record at a field level

# Key Concepts to Remember

- Data Exchange Agreement
- Partner Data Retention (Minimum Necessary)
- Access Control
- Data Repository
- Data Breach/Data Loss
- Patient Consent
- Partner Compliance Measurements

# Questions?

Richard Chapman

[richard@informationinventory.com](mailto:richard@informationinventory.com)

502.316.0828