

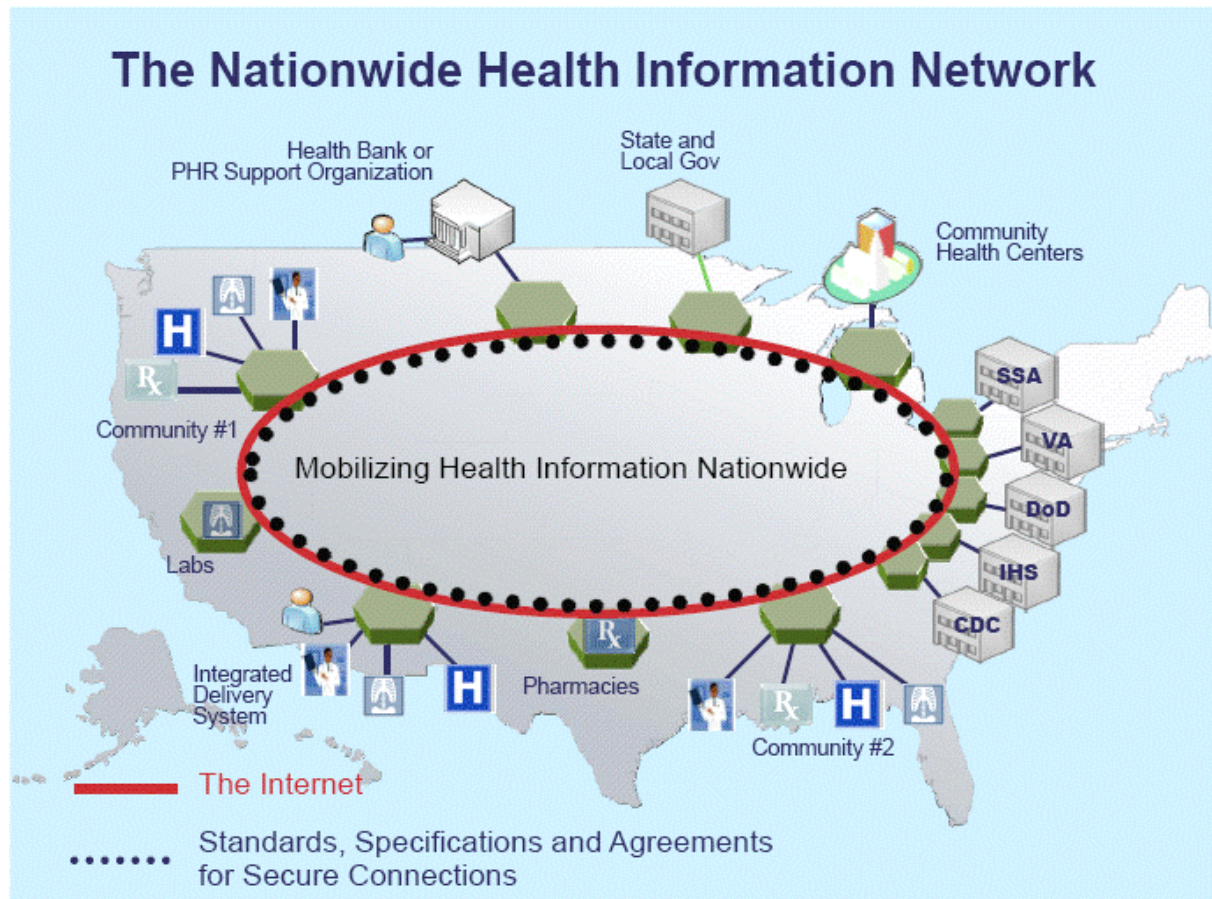
Privacy and Security Challenges to Electronic Health Information Exchange

Linda Dimitropoulos, PhD
Director of Health Services Research
Survey Research Division
April 28, 2009

Overview

- National vision for health information exchange
- Concept of privacy in the context of HIE
- Real and perceived risks and concerns
- Current state of privacy protections
- Need for “policy interoperability”
- The HISPC Model: A bottom-up approach
- Path Forward

The National Vision

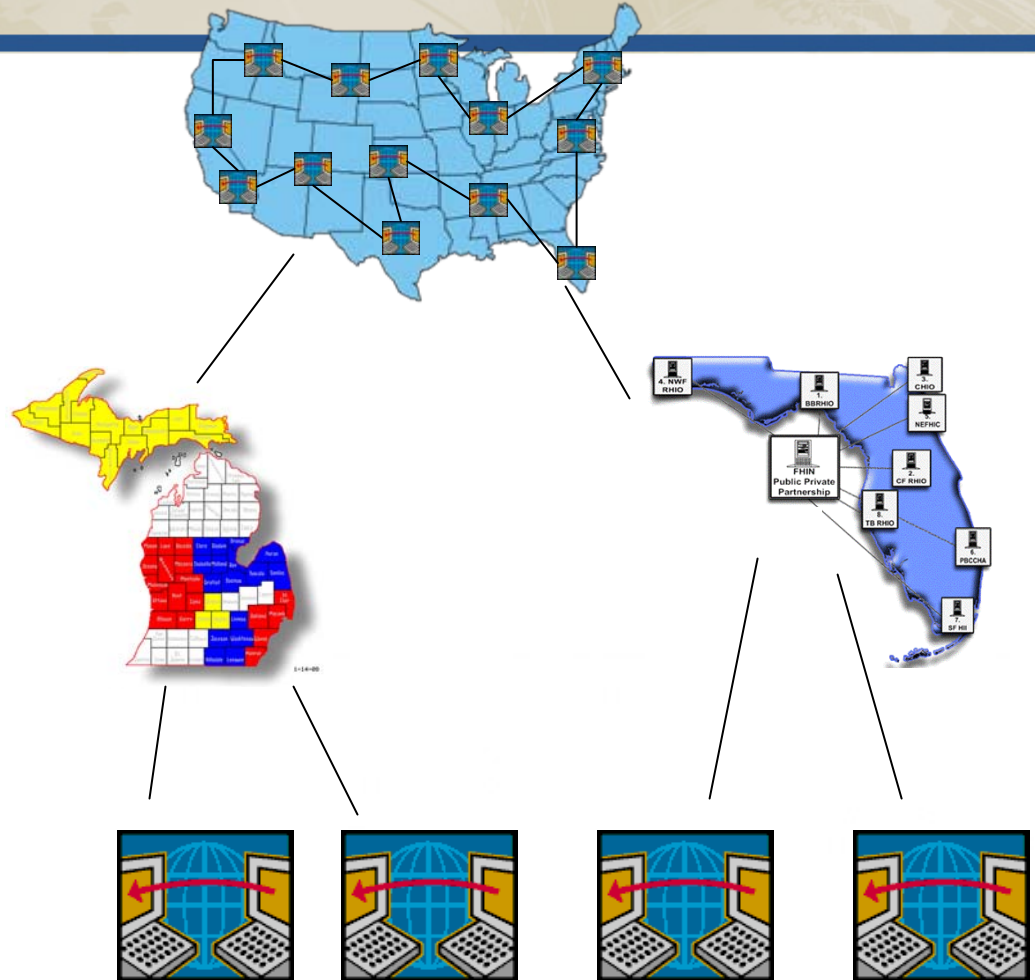


Basic Components of Exchange

Nationwide Health Information Network

Health Information Exchanges

Electronic Health Records and Personal Health Records



Concept and Definition of Privacy

“The claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others.” --Alan Westin

Commonly Cited Concerns Related to the Privacy of Health Information

- Health care consumers
 - Discrimination in employment, insurance or access to credit
 - Medical identity theft
 - Personal relationships/embarrassment
 - Unauthorized secondary uses such as marketing and fundraising
 - Having control over how their information is used
- Providers and clinicians
 - Compliance (potential liability, cost)
 - Patient record matching
 - Liability for wrongful disclosure
 - Concerns about data quality
 - Having access to “all” of the data

Current Protections

- HIPAA Privacy rule provides a federal floor of protection
- 42 CFR pt 2 regulates use and disclosure of patient information regarding alcohol or drug abuse
- CLIA, FERPA, etc
- Most states have laws that are more stringent than the federal laws

Current Landscape

- “In a paper-based system, privacy is currently protected by chaos.” –Mark A. Rothstein
- Variation in privacy and security business practices and policies creates a barrier to electronic clinical health information exchange
- The existing paradigm for privacy and security protections does not fully accommodate active consumer participation in health information exchange

Health Information Security and Privacy Collaboration (HISPC)

- Established by RTI in 2006 through a contract with AHRQ and ONC
- Began with 34 states and territories and expanded to 42 states and territories
- A single organization was designated by the Governor of each state to represent the state or territory in the collaboration
- Established a nationwide network of stakeholders to develop common solutions to privacy and security challenges

Goals

- Preserve privacy and security protections but in a manner consistent with interoperable electronic health information exchange
- Incorporate state and community interests, and promote stakeholder identification of practical solutions and implementation strategies through an open and transparent consensus-building process
- Leave behind in states and communities a knowledge base about privacy and security issues in electronic health information exchange that endures to inform future HIE activities

Tasks

- Assess the variations in organization-level business practices, policies and state laws that create a barrier to eHIE
- Develop a range of feasible solutions and a plan to implement the solutions
- Work in multi-state collaboratives to prevent the creation of silos

Sources of Variation: Federal

- Which regulation applies and under what conditions?
 - HIPAA Privacy Rule - multiple interpretations and applications
 - HIPAA Security Rule - confusion about the different types of security required
 - 42 CFR pt 2 – differences in language and drivers between HIPAA and 42 CFR pt2 create ambiguity
 - CLIA, FERPA



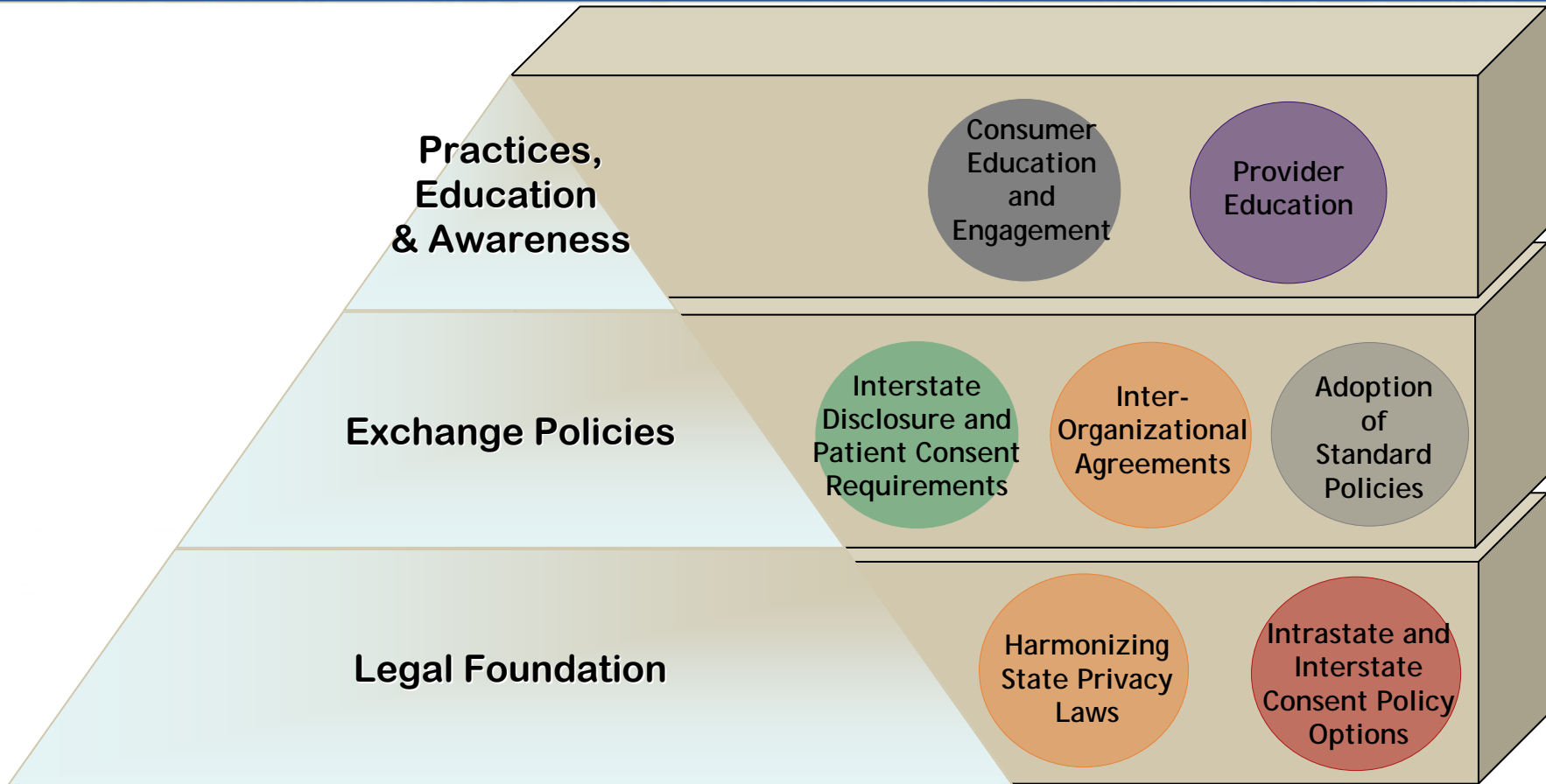
Sources of Variation: State

- State Privacy Law
 - When does it apply and under what conditions?
 - Fragmented and scattered throughout many chapters of code
 - Conflicting
 - Antiquated and not applicable to eHIE

Variation in Consent for Disclosure for Treatment

- Lack of understanding about when federal and state laws require patient consent for disclosure
- Lack of a standardized requirement for when to use patient consent for disclosure
- Lack of a standard “form” to be used to obtain and manage patient consent for disclosure

The HISPC Model



Practices, Education and Awareness: Consumer Education & Engagement

- **A wealth of resources**
 - Glossary of Terms
 - Compendium of Consumer Resources
 - Guidelines for Literacy & Language Considerations
 - Health IT FAQs
 - Communication Strategies
 - Media Materials
 - Documentaries
 - Websites
 - Education Toolkits



Practices, Education and Awareness: Providers

Physician to physician messages

- Electronic
- Face-to-face



HEALTH INFORMATION SECURITY & PRIVACY **TOOLKIT**

Key Message Elements

- Benefits of electronic health information exchange
- Best practices for security and privacy
- “It’s Safe, It’s Secure, It’s Time”

www.Secure4Health.com

Provider Education (continued)

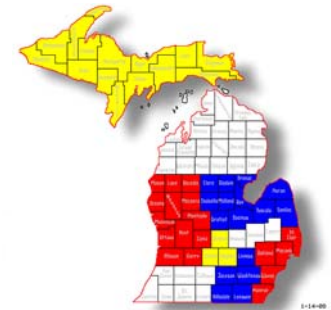
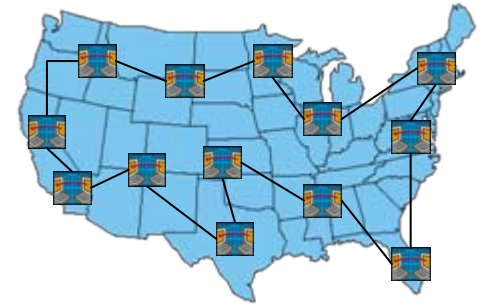
- Power Point Presentations
- Brochures
- Stand-up banners for conferences
- Newsletter and Journal articles
- Press Releases
- Interactive Website & videos by:
 - Dr. John Halamka, HITSP
 - Dr. David Kibbe, AAFP ,
 - Dr. Mark Leavitt , CCHIT
 - Dr. Daniel Mongiardo, Lt Gov, State of KY
- Links to free CMEs
- E-blasts with news updates

Found at www.Secure4Health.com



HISPC Impact at all Levels

- Pushed issues and potential remedies to the federal level
- Identified areas for harmonization at the state-level and tools to facilitate the process
- Developed standard policies and inter-organizational agreements for use at the HIE level
- Developed and disseminated education and outreach programs at the local organization, provider and consumer level



HISPC – Next Steps

- Innovations and Challenges
 - Focusing nationwide on education and outreach in each state
 - Multistate Collaboratives are expanding the work on harmonization of state law, common policy development, inter-organizational agreements.

Reports and Materials

www.rti.org/hispc

<http://healthit.ahrq.gov>

Thank you!