

2009 HISPC Seminar Series

Health Information Security and Privacy Collaboration (HISPC) Multi-State Collaboration

Using the Tools Developed by the Adoption of Standard Policies (ASP) Collaborative

June 23, 2009

Presenters:

John Lynch, Connecticut

Chris Doucette, Virginia

Jordana Huchital, Washington

Mary Crimmins, Ohio

Kim Snyder, Arizona

Art Davidson, Colorado

Moderator: Linda Dimitropoulos (RTI)

Health Information Security & Privacy

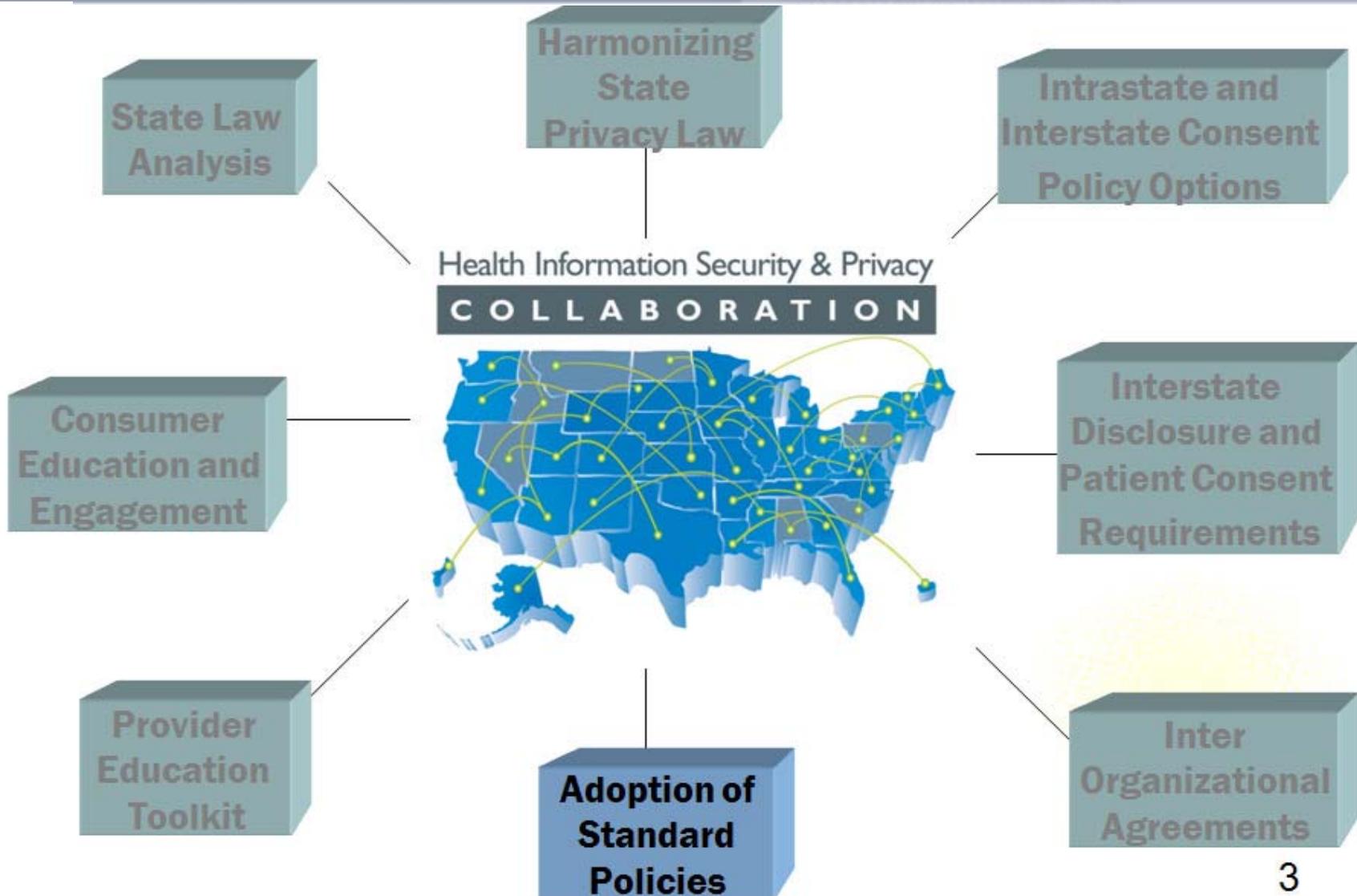
COLLABORATION



Before we begin...

- All participants are in audio broadcast mode—you must enable your computer speakers to listen to today's presentation.
- If you experience any difficulty with the audio, please notify the Webex Producer.
- If you have a question during the presentation, please send it in the Q&A box in the bottom right corner. At the end of the presentations, there will be a question and answer period.
- Please e-mail privacy.security@rti.org if you have any questions following this presentation.
- All HISPC materials can be found on the Web: <http://healthit.hhs.gov/HISPC>

HISPC Phase III



Session Agenda

- Learning Objectives
- Background
 - Who is ASPC?
 - Statement of the Problem
 - Project Goals
- Project Tools and How to Use Them
 - Uniform Security Policy
 - Guide to Adoption of Uniform Security Policy
- Lessons Learned/Next Steps

Learning Objectives

At the conclusion of the presentation, you will be able to:

Recognize and understand the role *privacy and security policies* play in establishing *trust* between entities for health information exchange to occur.

Utilize the Guide to Adoption of Uniform Security Policy to review, assess, adapt, and eventually adopt your own health information organization policies.

Background: Who We Are

Ten ASPC Participating States:

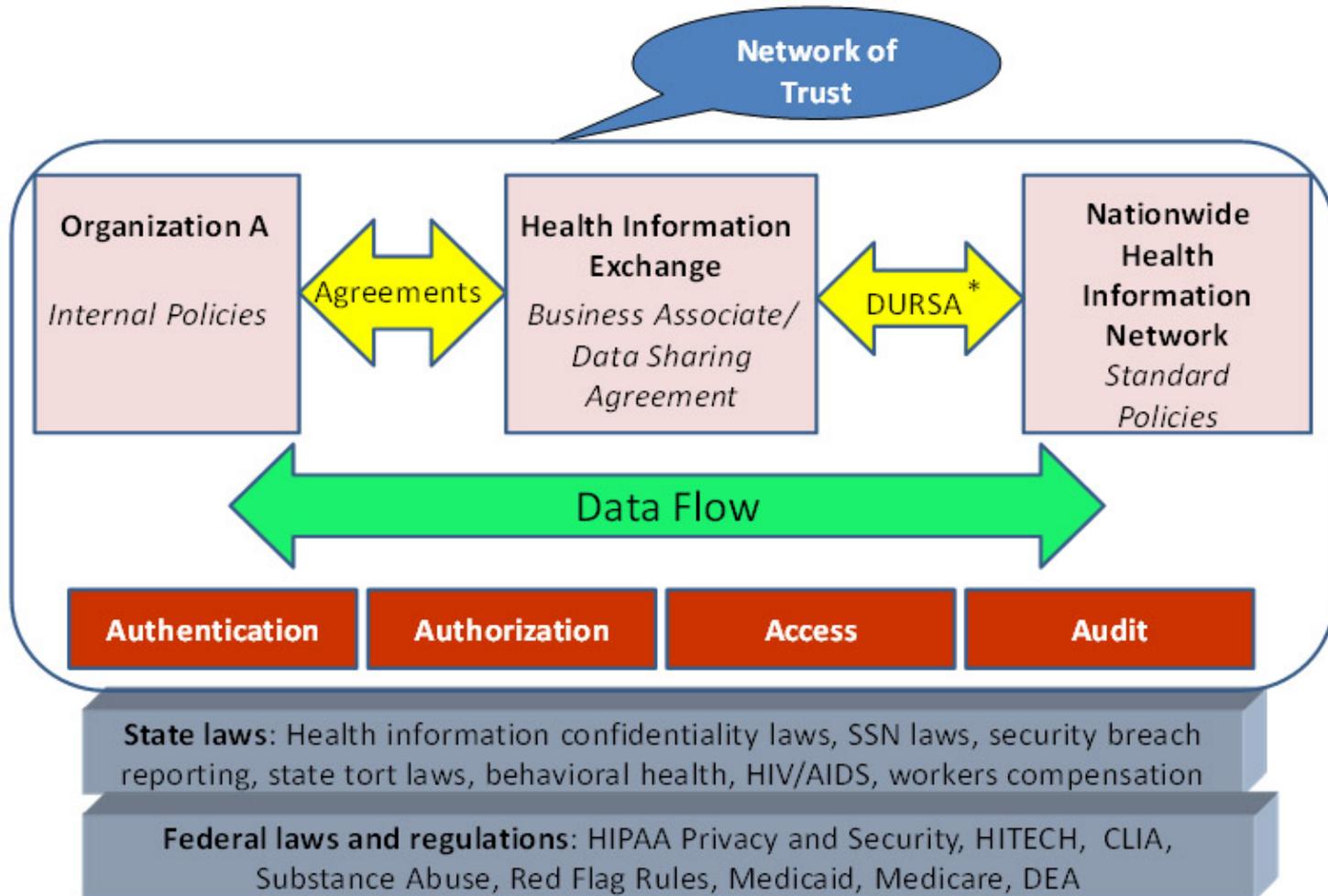
- Arizona: Kim Snyder,** Kristen Rosati, Emilie Sundie
- Colorado: Arthur Davidson
- Connecticut: John Lynch,** Lori Reed-Fourquet
- Maryland: David Sharp
- Nebraska: David Lawton, Anne Byers, Ann Fetrick
- Ohio: Mary Crimmins, Philip Powers
- Oklahoma: Ann Chou, Lynn Puckett
- Utah: Francesca Lanier
- Virginia: Chris Doucette, Kim Barnes, Reneé Kelley
- Washington: Jeff Hummel, Jordana Huchital
- Consultants: Chris Apgar, Gary Christoph
- RTI Liaison: David Harris

** Co-Chair

Polling Questions

- What kind of organization are you with?
(Choose all that apply)
 - Individual health organization
 - HIO / RHIO
 - State or federal agency
 - Application (software) vendor
 - Consultant
 - Other
- What role do you play in your organization?
(Choose all that apply)
 - Technical
 - Administrative
 - Privacy and security officer
 - Governance
 - Provider / caregiver
 - Other

Operationalizing Trust: HIE Legal and Security Context



*Data Use and Reciprocal Support Agreement

What Are the Issues?

- Health information organization (HIO) business models have ***dissimilar privacy and security practices*** .
- Practical HIO ***interoperability requires agreement*** on system behavior.
- A ***multitude of processes*** to authorize patient health information requests.
- Variation across ***user/entity verification*** methodologies.
- Policy requirements for ***authenticating users and audit differ*** by strategies.
- Unspecified ***enforcement methods*** persist.
- ***Alignment of varied policies*** that intersect and interact in complex ways.

ASPC Project Goals

Goal 1: Common Authentication Policies

- Trading partners trust in the process for **authentication** of user, organization, and system identity.

Goal 2: Common Audit Policies

- Participating members trust the **audit** policies of trading partners are sufficient to assure accountability.

Challenge: To Build Scalable Trust

Solution: Uniform Privacy and Security Policy



Why Is This Important?

As part of the Health Information Technology for Economic and Clinical Health (HITECH) Act, the Office of the National Coordinator for Health IT is required to update its strategic plan to include specific objectives such as:

SEC. 3001. OFFICE OF THE NATIONAL COORDINATOR

- Incorporation of **privacy and security protections for the electronic exchange** of an individual's individually identifiable health information.
- **Ensuring security methods to ensure appropriate authorization and electronic authentication** of health information and specifying technologies or methodologies for rendering health information unusable, unreadable, or indecipherable.

Tools

ASPC Glossary: Key Definitions

Minimum policy requirements

The policy requirements the ASPC developed through extensive individual state review of current policy and the subsequent comparison and negotiation of these requirements across the 10 states in the collaborative. These minimum policy requirements became the *framework* across which the Uniform Security Policy was built.

Uniform Security Policy

An aggregated set of policies that the ASPC recommends organizations adopt as a minimum policy to allow for interoperability with other organizations for health information exchange.

The Uniform Security Policy (USP)

What is the Uniform Security Policy?

Digital Policies * Model Agnostic * Standards-based * Negotiated

Scope:

Authentication of a provider access to the HIO for treatment and audit of access

Intended use:

Cross-entity exchange

Policy Status

- Publicly vetted
- Negotiated by six states
- Legal review
- Part of HIMSS interoperability showcase
- Undergone initial testing
- Ready for additional testing, evaluation, and adoption

NOTE: The Uniform Security Policy is not intended to cover all security policy areas of an HIO.

Key Authentication and Audit Features

Authentication		
Use Agreement <ul style="list-style-type: none"> Information is true, complete, and accurate Agree to comply with federal and state laws Act in good faith and be truthful at all times Access and use information only as permitted Confidentiality, integrity, and accessibility will be reasonably ensured 	Identity Management <ul style="list-style-type: none"> Unique identifier Affiliation Role 	
Audit		
Audit log data elements <ul style="list-style-type: none"> Unique Universal ID of viewer Role Data elements viewed, created, modified, deleted, or transmitted Date and time/duration of access 	Audit reports <ul style="list-style-type: none"> Routine scheduled reports Routine surveillance Ad hoc reporting by request or on suspicion of inappropriate access 	Enforcement <ul style="list-style-type: none"> Common policy on enforcement necessary for public trust of HIE, regulatory compliance and limiting legal risk.

Uniform Security Policy: Authentication

Section 1: Use Agreement

1.1 Requirement – Use Agreement

Section 2: Identity Registration

2.1 Required Data Set for Authentication

- 2.1.1 Data Source
- 2.1.2 Provider Identity Attributes
- 2.1.3 Organization Identity Attributes
- 2.1.4 Identity Attributes of the Data Source System

2.2 Role-based Access

- 2.2.1 Role

Section 3: Verifying Identity

3.1 Processes Used to Verify Identity

- 3.1.1 User Authentication
- 3.1.2 Organization Authentication
- 3.1.3 System Authentication

3.2 Variations Based on Type and Location of User

- 3.2.1 User Identity, Role, and Affiliation Verification
- 3.2.2 Signature Verification
- 3.2.3 Assurance Level
- 3.2.4 Relationship to Patient
- 3.2.5 Threshold Calculation
- 3.2.6 Digital Signature
- 3.2.7 Persistence

Section 3: Verifying Identity (continued)

3.3 Accommodations for Cross-HIE Verification and Data Integrity

- 3.3.1 Restricted Data Sharing and Data Integrity
- 3.3.2 Authenticate Recipient Identity (Organization / System / User)
- 3.3.3 Required Elements for Matching
- 3.3.4 Matching Criteria
- 3.3.5 Digital Signature
- 3.3.6 Persistence
- 3.3.7 Data Authentication
- 3.3.8 Data Validation
- 3.3.9 Type of Requestor
- 3.3.10 Signature Purpose

3.1.1 User Authentication

The methods for user identity vetting include both verifying the identity in person by a trusted authority and verification through the use of a demonstrated government-issued ID. The trusted authority is recognized by the state or federal government.

An applicant requesting an identity tied to a regulated provider type must have provider licensure validation.

Uniform Security Policy: Audit

Section 1 – Logging and Audit Controls

1.1 Log-in Monitoring

1.2 Information Systems Review

1.3 System Review

1.4 Security Audit Practices

1.5 Audit Trail and Node

Authentication (ATNA)

Section 2 – Periodic Internal Compliance Audits

6.5 Data Validation

For the purposes of data validation, the signer credentials must be from a trusted authority, and the credential must be current and without constraints, and the credential must be of the appropriate type for the requested data (for example physician or pharmacist). To ensure data integrity, credentials shall indicate that no change has occurred since the signature was applied and must have a valid date/time stamp.

Section 5 – Need to know Procedure/ Process for Personnel Access to Personal Health Information

5.1 Information Request

5.2 Audit Log Process

5.3 Data Authentication

5.4 Preparing a Query Message

Section 6 – System Capabilities

6.1 Audit Controls

6.2 Audit Log Content

6.3 Information Integrity

6.4 Data Authentication

6.5 Data Validation

Uniform Security Policy: Example

2.1.2 Provider Identity Attributes

The HIO will collect the attributes as needed for unique identification of the individual accessing the information in the HIO. Required elements are profession, role, name, the practice address (not home address), identity service provider and organization affiliation, business/legal address and License/ID. Other attributes that are required, if they exist for this individual includes:

- Specialization/specialty,
- Email address
- National Provider Identifier (NPI), and
- Digital Identity *DAT10*

DAT 10 Requirements also considered:

Directory of all HIOs

Included in the directory: Contact fax numbers

Master provider index to query by provider for a specific patient

AUT *, AUD *, DAT *, SYS *, POL * - refers to a negotiated minimum policy requirement and can be referenced the Cross State technical source document.

Guide to Adoption of Uniform Security Policy

Purpose

Provide a method for entities to review and adopt the Uniform Security Policy.

Provide a framework that extends the review to additional policies.

Guide to Adoption of Uniform Security Policy

Audience

- Individual organizations
 - HIOs, RHIOs
 - State Agencies



Context for Using the Guide



Stage of Policy Development



Polling Questions

- **Do you already have formal, written policies in place for authentication of users and/or audit?**
 - Yes
 - No
 - N/A

- **If you do have policies, what is the scope of these policies?**
 - Within an individual organization— internal only
 - Across organizations
 - Both (within and across)

The Adoption Process: Summary



The Adoption Process: Goal/Scope

What is the goal for this process?

- What are you trying to achieve?
- Adopt Uniform Security Policy

What is the scope?

- Authentication and audit of a health care provider for treatment purposes
- Which use case is used?
- What is the business model and architecture?

The Adoption Process: Resources

What team resources are available for this project?

- Types of resources

Who are the stakeholders?

- How to get stakeholders involved

Business Process Analysis and Desktop Review

Are authentication and audit policy already in place?

What is the business process you are trying to resolve?

How will you measure the risk associated with the business process?

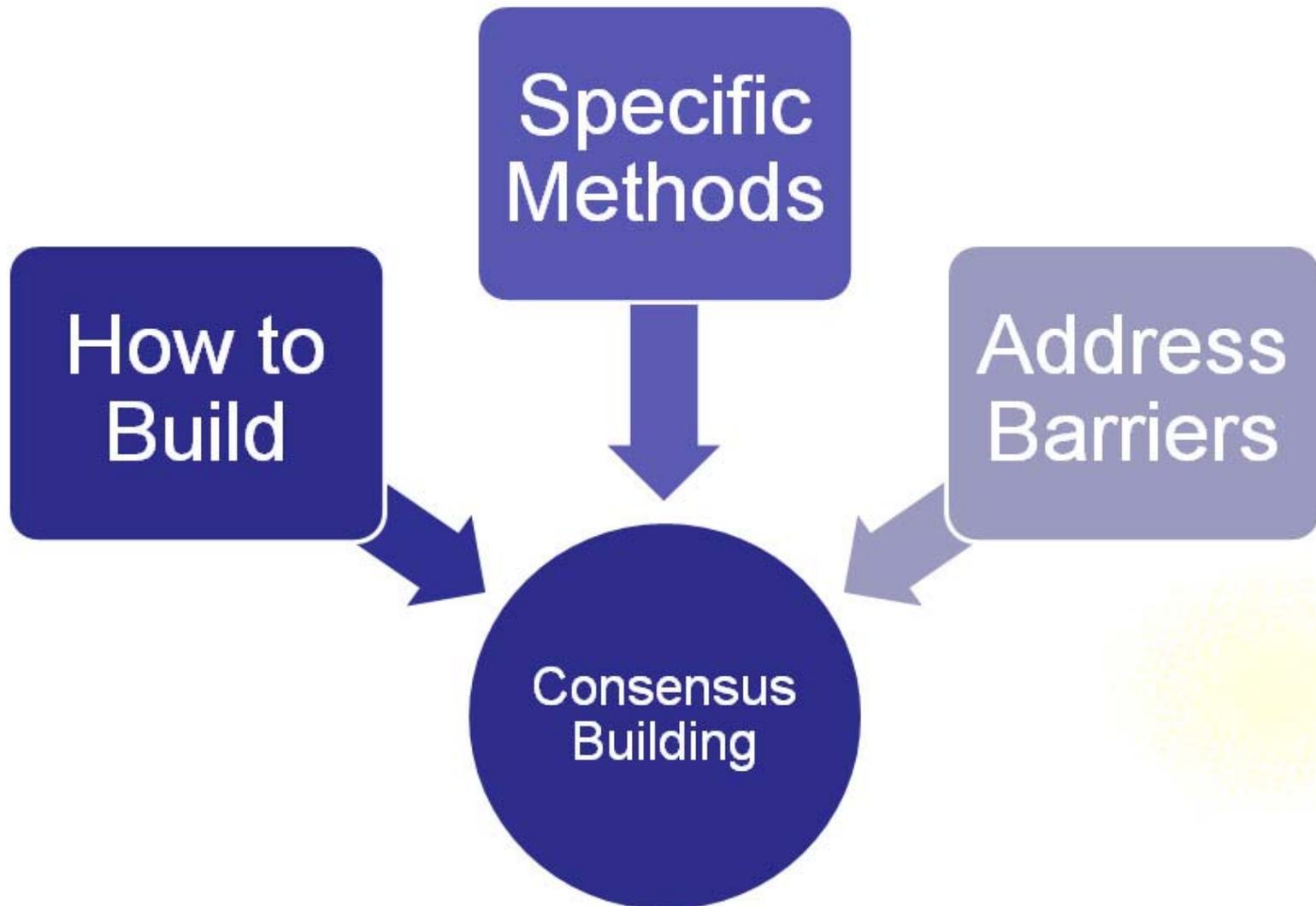
Business Processes: No Policy in Place

Actor	Event	Authentication / Audit Requirement	ASPC Recommended Basic Policy Requirement	Issues	Resolution
Clinician	Laboratory results for a patient	<p>Clinician is identified by the trusted authority</p> <p>Clinician logs into system using password and login name</p>	<p>Authentication Section 3 – Verifying Identity</p> <p><u>3.1.1 User Authentication</u></p> <p>HIO use of a specific naming convention as a primary identifier is required with a minimum assurance level used of Medium (knowledge/strong password/shared secret).</p>	Current system only allows for password	Upgrade system security to allow for shared secret
HIO	List and review of people accessing the HIO	HIO must be able to audit access to the HIO by providers	<p>Audit Section 1 – Logging and audit controls</p> <p><u>1.1 Log-in Monitoring</u></p> <p>Audit log is required and must be reviewed on a regular basis.</p>	No issue	NA

Desktop Review: Policy in Place

Uniform Security Policy Requirements	Local Policy	Gaps	Recommendation	Solutions
<p>Authentication Section 1- Use Agreement <u>1. Use Agreement</u> Health Information Organizations should have a data sharing agreement with participating providers that defines the privacy and security obligations of the parties participating in the HIO. These agreements should require the use of appropriate authentication methods for users of the HIO that depend on the users' method of connection and the sensitivity of the data that will be exchanged.</p>	Local one-to-one contracts	Stricter than minimum	Accept a less strict policy for cross-state sharing only	Allow for cross-state sharing of HIE
<p>Authentication Section 2- Identity Registration <u>2.1 Required Data set for Authentication</u> A directory of data sources within the target HIO is required, and includes primary contact information of registered members, identity attributes of providers, organization and systems.</p>	Same	None	Accept minimum policy requirements	—

The Adoption Process: Consensus Building



The Adoption Process: Legal Assessment

Federal

- How to ensure HIPAA compliance
- HITECH Act
- CLIA regulations
- Federal substance abuse treatment

State Laws

- Laws that may impact exchange of certain information

State Legislation

- Change existing state law
- Introduce new state law

The Adoption Process: Documentation of Policy

Documentation

End
Users

Technical
Team

Example of Technical Documentation

Policy Statement	Technical Specification	Date Completed	Issues Reported
<p>Authentication Section 2 -Identity Registration <u>2.1.2 Provider Identity</u> The HIO will collect the attributes as needed for unique identification of the individual accessing the information in the HIO. Required elements are profession, role, name, practice address, business/ legal address and License/ID.</p>	<p>Coding must include a role.</p>	<p>Ex. 2-27-10</p>	<p>Custom code required to add field for role.</p>
<p>Audit Section 6 – System Capabilities <u>6.4 Data Authentication</u> For purposes of data authentication the use of a valid date/time stamp is required.</p>	<p>Coding of the system and the audit reports must include the valid data / time stamp required. Data stamp needs to print on the audit report.</p>	<p>Ex. 3-5-09</p>	<p>Audit report doesn't include time of access.</p>

The Adoption Process: Implementation

Testing

- Functional
- Regression
- System
- Integration
- Load

Training

- State Government
- Health Information Organizations
- Provider Community
- Consumer Community

The Adoption Process: Implementation (cont.)

Deployment

- Go Live
- Support
- Issues tracking

Production

- Analysis of issues
- Effectiveness of policy
- Evaluation of changes in workflow and/or systems

Anticipated Challenges and Recommended Mitigation Strategies

	Anticipated Challenge	Mitigation Strategy
BUSINESS	Local or regional solutions do not conform to national standards	Educate member organizations on standards and the benefits of standards
LEGAL	Granularity of audit logs are not adequate for reports	Evaluate system triggers; implement more granular data capture
POLITICAL	Lack of transparency	Educate the stakeholders; develop a web site for documentation and dissemination.
TECHNICAL	Varying authentication practices	Define the minimum requirements by adopting the standard policies.
EDUCATIONAL	Policy implementation requires legislation or regulation	Prepare whitepapers identifying models. Provide proposed statutory or regulatory language to the legislature or regulating body.
GOVERNANCE	Policy conflict in member organizations	Specify mechanisms to be used in conflict resolution as part of the legal agreements.

Guide to Adoption of Uniform Security Policy: Appendices

A. Appendix A: Feasibility: Preparing for Change and Process Checklist

Section 1: Preparing for Change

Section 2: Checklist

B. Appendix B: Uniform Security Policy

C. Appendix C: Other Useful Resources

D. Appendix D: Glossary and Abbreviations

E. Appendix E: References

F. Appendix F: Contributors

Guide to Adoption of Uniform Security Policy: Appendices

Appendix A: Feasibility: Preparing for Change



Guide to Adoption of Uniform Security Policy: Appendices

To use this framework to prepare for change, consider the following:

Is your organization prepared to assure **communication** among organizational members as the central focus of all steps in the change process?

- ▶ Transparent
- ▶ Across many organization levels
- ▶ Develop respect for the input of all
- ▶ Organizational structure is important in facilitating the communication

Does your organization have the **knowledge** that it needs to implement minimum security standards for health information exchange?

Is your organizational leadership **persuaded** to pursue this change to implement minimum security standards for health information exchange?

Is your organizational leadership **adopting** minimum security standards for health information exchange?

Is your organizational leadership prepared to **implement** minimum security standards for health information exchange?

Guide to Adoption of Uniform Security Policy: Appendices—Process Checklist for Feasibility

Goal and Scope		
	<input checked="" type="checkbox"/>	Notes
Consider Pre-existing Structure		
Determine if this is an existing health information organization (HIO) or if an HIO is being planned		
If the HIO exists, what level is it organized at:		
Local		
Sub state region		
Sub state region that crosses state lines		
State		
Multi-state		

Goal and Scope Milestones

- ▶ Document the business model of the Health Information Organization
- ▶ Collect and analyze existing agreements
- ▶ Establish a privacy, technical security and administrative/business security

Lessons Learned

Be pragmatic: The perfect is the enemy of the good.

Present reality limits the specificity of policy.

Plan to improve and extend the policy.

Authentication, Authorization, Access, and Audit are not separable; they provide emphasis.

Lessons Learned

A significant undertaking in an uncharted domain

Need for clearly defined scope and methodology –
with continuous monitoring of scope

Limitations of consensus-based decision making

Policies cannot be static if they are to address the
changing landscape of health information exchange

Lessons Learned

A significant undertaking in an uncharted domain

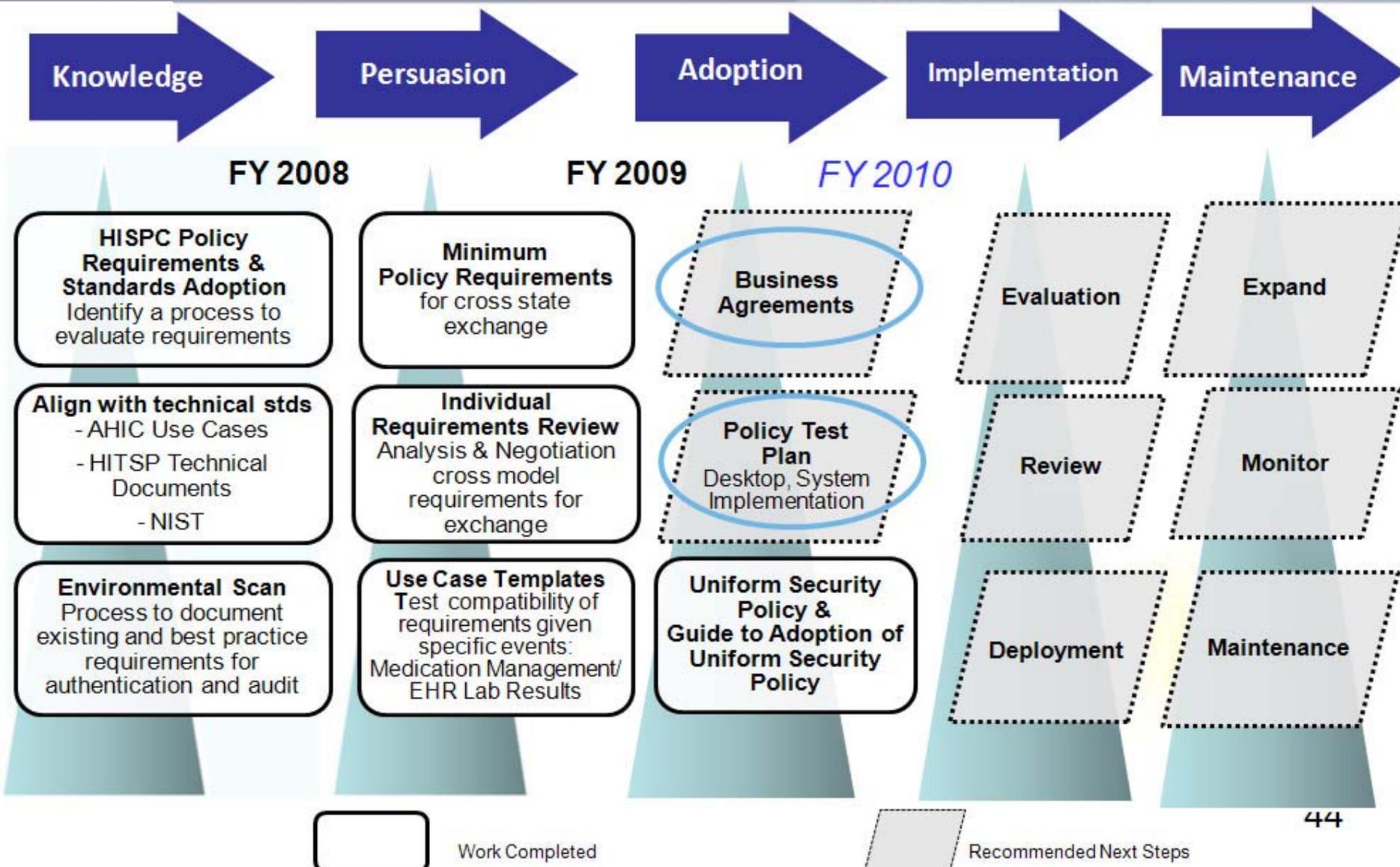
Need for clearly defined scope and methodology – with continuous monitoring of scope

Limitations of consensus-based decision making

Policies cannot be static if they are to address the changing landscape of health information exchange

Because things are the way they are, things will not stay the way they are. ~Bertold Brecht

Next Steps



Recap

Incorporate feedback from lessons learned.

Expand the use cases and types of transactions.

Extend into: authorization, access, and other areas.

Broaden the policy-vetting process and certification of systematic policy adoption.

Determine strategy to simultaneously support NHIN and multi-state engagements while establishing effective minimum policy thresholds.

Fund prototypes and track results to share broadly.

Polling Questions

Based on this presentation, how likely are you to embark upon the process of to review, evaluate, adapt, and adopt the Uniform Security Policy?

- Very likely
- Likely to review and adopt the Uniform Security Policy
- Neutral
- Unlikely
- Very unlikely
- Not applicable based on my organization and/or role

Questions?



Contact Information

Kim Snyder

kim.snyder@illumineITSolutions.com

602-321-1066

John Lynch

jlynch@ProHealthMD.com

860-284-5288

Chris Doucette

chris.doucette@dmas.virginia.gov

804-371-6326

David Harris

dharris@rti.org

919-541-7493

Mary Crimmins

mary.crimmins@wright.edu

937-671-9058

Jordana Huchital

jordana@interactiveoutcomes.com

206-354-0718

Art Davidson

adavidson@dhha.org

303-436-7364



Thank You for Attending

- Please visit <http://healthit.hhs.gov/HISPC> for full access to all of the products discussed today as well as information about the other HISPC collaborative products.
- Additional materials are being posted as they become available throughout the months of June and July.