


Health Information Security and Privacy Collaboration (HISPC) Adoption of Standard Policies Collaborative (ASPC)

Adoption of Uniform Security Policy

**HIMSS
Showcase Presentation
April 6, 2009 4:15 pm**



1

Health Information Privacy and Security Collaboration (HISPC)

- Funded by the US Dept of Health and Human Services
Office of the National Coordinator for Health Information Technology
- Managed by RTI International
- Nationwide in scope: 42 states and territories
- A single entity within each state and territory, endorsed by the governor, represents each state, develops feedback from local stakeholders
- Collaborative efforts to identify common solutions to security and privacy issues related to electronic health information exchange (HIE)

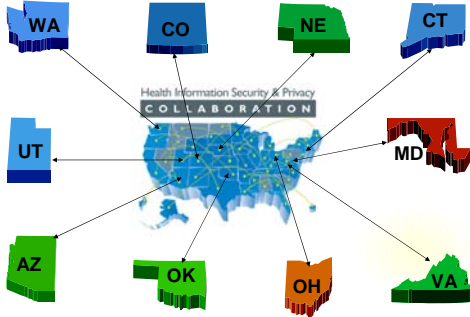
2

Composition of HISPC Collaboratives

Collaborative:	States and Territories:
Interstate Disclosure and Patient Consent Requirements	IN, ME, MA, MN, NH, NY, OK, RI, UT, VT, WI
Inter/Intrastate Consent Policy Options	CA, IL, NC, OH
Harmonizing Privacy Law	FL, KY, KS, MI, MO, NM, TX
Consumer Education and Engagement	CO, GA, KS, MA, NY, OR, WA, WV
Provider Education	FL, KY, LA, MI, MO, MS, TN, WY
Adoption of Standard Policies	AZ, CO, CT, MD, NE, OH, OK, UT, VA, WA
Inter-organizational Agreements	AK, GU, IA, NJ, NC, SD

3

HISPC Adoption of Standard Policies Collaborative



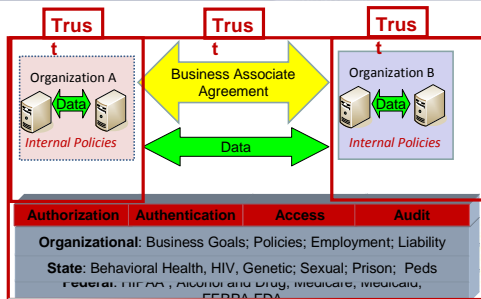
4

Issues

- Different Health Information Organization (HIO) business models have dissimilar privacy and security practices.
- Practical HIO interoperability requires organizations to agree on system behavior and data retrieval/presentation responses.
- The multitude of processes currently used to authorize patient health information requests.
- Variation across user/entity verification methodologies.
- Policy requirements for authenticating users differ by state
- Enforcement of the basic policy requirements.
- Alignment of efforts is essential as various policy areas interact and touch each other in complex ways.

5

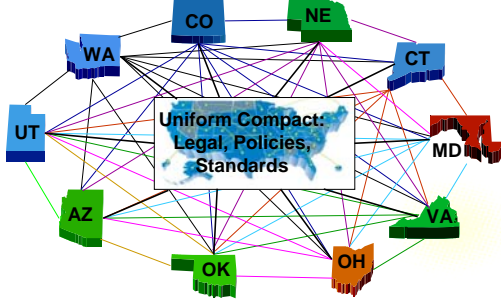
Current Network of Trust



6

Challenge: How to Build Scalable Trust?

Solution: Uniform Privacy and Security Policy



ASPC Approach

- Scope
 - Policies for Authentication & Audit
 - Focus on provider access and HIE for treatment purposes
- Ten states, local business cases to incorporate variation state in requirements and need
- AHIC Use Cases to simulate information flow and build off standards
 - Medication Management
 - Lab Result
- State Stakeholder community feedback
- Implementation Guide to support adoption

8

ASPC Methods

- Perform Baseline Environmental Scan for each participating state
 - Begin Building Glossary – Negotiate terms
 - Begin Building Policy Templates
 - Identify Local Policy Requirements
 - Identify Existing Tools: (AHIC Use Cases, IHE, HITSP, Markle, NIST)
- Create AHIC Use Cases Requirements Templates
- Complete Use Case Template by state
- Aggregate and compare
- Negotiate
- Build Policy
- Stakeholder Review
- Guide to Adoption

9

Uniform Security Policy for Authentication and Audit

Authentication Policy

(27 requirements)

- Use Agreement
- Identity Registration
- Verifying Identity
- Identity Provisioning
- Identity Maintenance

Audit Policy

(20 requirements)

- Logging and Audit Controls
- Periodic Internal Compliance Audits
- Information Access
- Need to Know, Establish Minimum Necessary for Data Management and Release
- Need to Know Procedure/Establish Process for Personnel Access to Protected Health Information (PHI)
- System Capabilities

10

Authentication Policy 3.1.1: User Authentication

3.1.1 User Authentication

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

An applicant requesting an identity tied to a regulated provider type must have provider licensure validation. It is acceptable that this occur along with the validation required of any employee of a licensed provider organization.

Also, the 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).

11

Audit Policy 5.1: Information Request

- The date and time of the request,
- The reason for the request,
- A description of information requested, including the data accessed, data transmission, any changes to the data (adds, changes, deletes), and whether the data were transmitted to, or printed by another party,
- The ID/verification of the party receiving the information,
- The ID of the party disclosing the information,
- The method used for verification of the requesting entity's identity.

12

Uniform Policy continued....

Accountability and Enforcement

- Termination of individual access
- Participating entity take disciplinary action for inappropriate access
- Termination of HIE agreement with participating entity
- Reporting compliance to HIO
- Mitigating impact of noncompliance on consumers

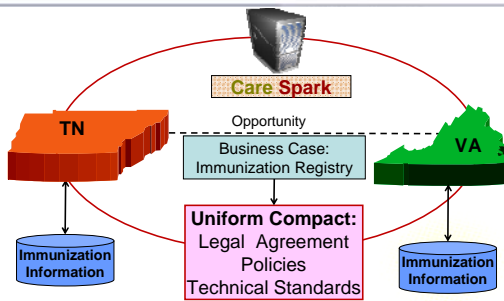
13

Organizational Adoption of Uniform Compact

- Inter-organization Agreement (Legal)
- Business Associates Agreement (HIPAA)
- System Specifications
- Technical Standards
- Uniform Policy Statement**
- Standard Terms/Glossary**
- Authentication Policy**
- Audit Policy**
- Authorization Policy
- Archive policy
- Disaster Recovery Policy
- ...

14

Creating Trust between Tennessee and Virginia



15

Upfront Encoding

- Enroll Identities (People, Entities)
- Authorize Affiliation
- Assign Role (Organizational, Functional, Structural)
- Categorize Information Asset Sensitivity
- Establish Transaction Purpose
- Encode Specific Information Sensitivity Rules
 - Patient Authorization Required
 - Role by Asset Sensitivity

19

Functional Testing of each module

AHIC Use Case Events/Actions Triggering DAT1 - Role	ASPC Uniform Policy	Action Required
3.5.2.1 Authenticate clinician requesting lab test result	2.2.1 Role Organization role required; functional role or structural role required.	Check for role in authentication process

20

Functional Testing: Lab Use Case Example

Laboratory Results Reporting Use Case Clinician

```

    graph TD
      subgraph Steps
        S220[3.2.2.0 Receive notification of lab test results]
        S221[3.2.2.1 Receive notification that test results are available]
        S230[3.2.3.0 Query for laboratory test results]
        S231[3.2.3.1 Submit Authentication information to locator system]
        S232[3.2.3.2 Clinician and locator system agree on patient identity]
        S233[3.2.3.3 Transmit request for specific lab test]
        S234[3.2.3.4 Receive the data repository location where the test results are stored]
        S235[3.2.3.5 Log interaction with locator service]
      end
      S231 --> UAP[User Authentication Policy]
      S233 --> AP[Audit Policy: Info Disclosure, Info Request]
  
```

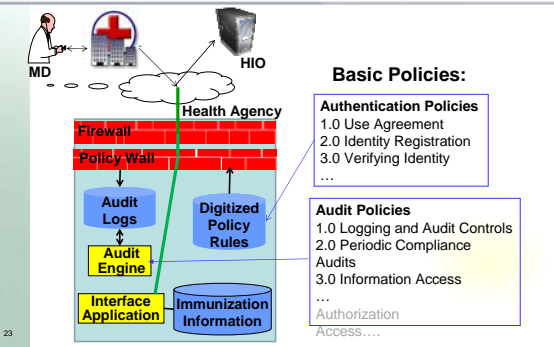
21

Unit Testing of all Application Modules

Actor	Information Needed	Authentication / Audit Requirement	ASPC Recommended Basic Policy Requirement	Issues	Resolution
Clinician	Laboratory results for a patient	Clinician logs into system using password and login name	3.1.1 User Authentication requires minimum assurance level of Medium (Knowledge, strong password/ shared secret) (see NIST e-authentication Pub. 800-63)	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	Section 1 – Logging and audit controls 1.1. Logging Monitoring Audit log is required and must be reviewed on a regular basis	No issue	

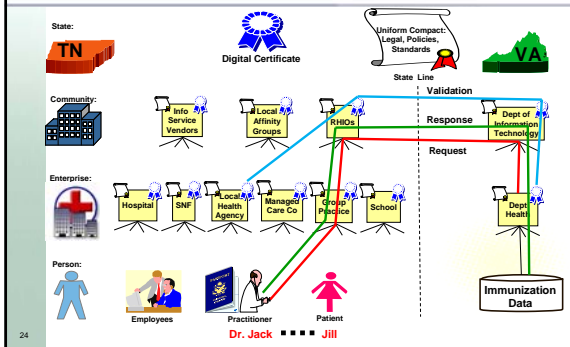
22

Integration Testing Across All Applications



23

Chain of Trust Enabled by Uniform Compact, Policy, Standards



24

Training, Deployment, Production, Maintenance, QA

- Maintain real time Identity management updates/revocations
- Monitor all Authentications
- Routine Audit of Logs
- Move toward higher level of policy agreement
- Policy recommendations
- Review of audit reports
- Audit of authorized users
- Review of system performance
- Security breaches
- Data quality review
- User access data reviewed

25

Next Steps

- Monitor/feedback progress and lessons learned
- Expand the use cases and types of transactions
- Extend into: authorization, access, disaster recovery, archives... policies
- Organize an HIO clearinghouse to inform about standard policy developments
- Broader policy vetting process and certification of system policy adoption (e.g., HIMSS and/or CCHIT)
- Determine strategy to simultaneously engage multiple states minimum standards:
- Fund prototypes and track results to share broadly
- Encourage vendors to incorporate capability and integrate with technical standards

26

Special Thanks to

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

27

Questions?

Health Information Security & Privacy

COLLABORATION



28
