

Unraveling Privacy and Security in HIEs:

An Overview of Requirements and Options for Medicaid/SCHIP Programs

Presented by:

**Joy Pritts, JD - Research Associate Professor, Health Policy
Institute, Georgetown University**

**Walter G. Suarez, MD, MPH - President and CEO, Institute
for HIPAA/HIT Education and Research**

Overview

- Welcome
- Before We Begin
- Introductions
- Part 1: *Overview of Privacy Requirements*
Presented by Joy Pritts, JD
- Part 2: *HIE and Information Security for Medicaid/SCHIP Agencies*
Presented by Walter Suarez, MD, MPH
- Question and Answer
- Closing Remarks



Before we begin...

- The Webinar will be recorded and the link to the recorded session will be distributed via email on Monday, March 24th.
- Please note all participants will be placed on mute once the presentations begin.
- If you have a question during a presentation, please send your question to the host through the chat. The host will notify the presenter and will read the question aloud.
- If you wish to be un-muted, choose the “raise hand” option to notify the host.

■ Listserv Registration

- Please register for the listserv to receive announcements about program updates
- To register go to <http://healthit.ahrq.gov/Medicaid-SCHIP>
- Click on “Medicaid-SCHIP Fast Facts” on the left-hand side of the screen
- There are two ways to register for the listserv:
 - 1. Click the link “[Click here to subscribe to the listserv](#)” which will open a pre-filled email message, enter your name after the text in the body of the message and send.
 - 2. Send an E-mail message to: listserv@list.ahrq.gov.
On the subject line, type: **Subscribe**.
In the body of the message type: **sub Medicaid-SCHIP-HIT** and **your full name**. For example: sub Medicaid-SCHIP-HIT John Doe.
You will receive a message asking you to confirm your intent to sign up.



Comments and Recommendations for Future Sessions

- Please send your comments and recommendations for future sessions to the project's email address:

Medicaid-SCHIP-HIT@ahrq.hhs.gov



PART 1
Overview of Privacy Requirements

Joy Pritts, JD
Research Associate Professor
Health Policy Institute
Georgetown University



Privacy Standards for Medicaid/SCHIP Agencies

- Medicaid/SCHIP confidentiality standards
- HIPAA Privacy Rule
- Federal alcohol and substance abuse regulations
- Other state privacy/confidentiality statutes and regulations (e.g., HIV/AIDS, mental health)



Interaction

- Rule of thumb, follow most restrictive requirements.



Medicaid & SCHIP Confidentiality Regulations

Confidentiality Regulation

- Medicaid and SCHIP programs must restrict the use or disclosure of information concerning applicants and recipients to *purposes directly related to plan administration.*

See § 1902(a)(7) of the Social Security Act; 42 USC § 1396a (a)(7)

42 CFR § 431.301; 42 CFR § 457.1110



Information Subject to Confidentiality Requirements

- Names and addresses
- Medical services provided
- Social and economic conditions or circumstances
- Agency evaluation of personal information
- Medical data, including diagnosis and past history of disease or disability
- Any info. received for verifying income eligibility and amount of medical assistance payments



Purposes Directly Related to Plan Administration Include

- Establishing eligibility
- Determining the amount of medical assistance
- Providing services for recipients
- Conducting or assisting an investigation, prosecution, or civil or criminal proceeding related to the administration of the plan.

Other Restrictions

- Access limited to persons or agencies that are subject to standards of confidentiality comparable to Medicaid/SCHIP program
- Agency must, whenever possible, obtain permission of the individual or family before responding to a request for information from an outside source (unless info. is to be used to verify income, eligibility, and amount of medical assistance payments)



Scope of Restrictions

- Apply to all requests for information from outside sources including other governmental bodies



Some Challenges in HIE

- Requirement for individual permission to respond to outside requests for information
- Scope of “administration of plan”
- Requirement that others receiving data be subject to confidentiality standards comparable to Medicaid/SCHIP standards

Obtaining Permission

- Meds-Info ED regional HIE for providing prescription data to emergency departments
- MA Medicaid provided eligibility and paid prescription history to emergency rooms for treatment in a upon ER's request
- Obtained individual consent



State Immunization Registries: Challenge

- Medicaid agencies in a number of states will not share immunization data with state-run immunization registries because this activity is not seen as a purpose directly related to administration of the Medicaid plan.



State Immunization Registries: Solution

- One state reported sharing Medicaid data under a data use agreement with state Dept. of Health contractor which collects and analyzes immunization data.



CMS Guidance *

Medicaid Directors Letter

“Facilitating Collaborations for Data Sharing
Between State Medicaid and Health
Agencies”

<http://www.cms.hhs.gov/SMDL/SMD/list.asp>

Under “Data Sharing Agreement”

Oct. 22, 1998

*Issued by Health Care Financing Administration, now known as CMS



CMS Guidance

- Aim to reduce barriers to sharing data between Medicaid and health agencies and to support innovative approaches to the design and implementation of State information systems
- Provides model data sharing agreement “to guide the permissible sharing and dissemination of Medicaid data among State Medicaid and Public Health agencies”



CMS Guidance

Benefits of sharing Medicaid data:

- Improving the technical capacity of States to analyze data from multiple sources to support policy decision making and program monitoring
- Promoting the development and implementation of common performance measures across multiple programs to improve their effectiveness
- To better utilize Medicaid encounter data to assist in public health surveillance to ensure appropriate care for the Medicaid population



CMS Guidance

- Weight
 - Provide clarification “on current information pertaining to Medicaid policy”
 - Ensure consistency

- Old
 - Has not been reaffirmed
 - Has not been revoked

- Could potentially seek clarification from CMS



HIPAA Privacy Rule

“Covered Entities”

- Health Plans

- Medicaid/SCHIP programs

- Most health care providers

- Health care clearinghouses

- Middlemen that process data into/out of standard data elements or format

“Protected Health Information”

- Information about a person’s past present or future health, health care or payment of health care;
- That can identify the person; and
- Was created or received by a covered health plan or health care provider

What Information Is Not Covered?

De-identified information

- Statistician has determined that risk is very small that info. could be used alone or in combination with other reasonably available info. to identify person who is subject of the information

- All 18 listed identifiers have been removed
 - Name
 - Address
 - Social Security Number
 - All dates (e.g., date of birth, date of treatment)
 - Others



HIPAA Privacy Rule: In General

- Creates rights for individuals with respect to their protected health information
 - See, get a copy of, and amend their health information
 - Receive a notice of privacy practice
 - Request limits on disclosures



HIPAA Privacy Rule: In General

- Prohibits use or disclosure of protected health information by a covered entity except as expressly permitted by the Rule or with the individual's authorization



Minimum Necessary

- Requires reasonable effort to limit information to minimum amount necessary to accomplish intended purpose.

Business Associates

Covered entity:

- May disclose protected health information to business associate *without* individual's authorization
- Must enter into a written agreement limiting the business associate's use and disclosure of information
 - Can be a memo of understanding

Business Associates

- Person or organization that performs functions *on behalf of* covered entity involving use or disclosure of identifiable health information
 - Examples: claims processing or administration, data analysis, processing or administration, billing, management, data aggregation, quality assurance etc.
- A covered entity can be a BA of another covered entity

Treatment, Payment & Health Care Operations

- In general, HIPAA does *not* require individual's written permission to use or disclose protected health information for these purposes
- Neither does it *prohibit* covered entity from obtaining such permission
 - Called “consent”



HIPAA Permits Use and Disclosure *without* Individual Authorization

For other listed purposes, subject to conditions

- Health oversight
- Research
- Judicial and administrative proceedings
- Other

Permitted Uses & Disclosures: Opportunity to Object

- Family or friends or others info. directly relevant to involvement with care or payment of care
- Disaster relief



Authorization

- Required for uses and disclosures not otherwise permitted by the Privacy Rule
- Must meet specific content requirements



Penalties

- Establishes civil and criminal penalties for covered entities that violate the requirements of the Privacy Rule
- Over 25,000 complaints have been filed and no fines have been imposed to date



HIPAA Interaction with State Law


HIPAA does *not* preempt a provision of state law that

- Substantially relates to the privacy of individually identifiable health information and
- Is *more stringent* than HIPAA
 - Prohibits or restricts use or disclosure allowed under HIPAA
 - More privacy protective of subject of identifiable info.



Some HIE Challenges


- How is a local HIE (RHIO) treated under HIPAA?
- What are the limits on sharing health information in a HIE?



HIEs (or RHIOs) Under HIPAA

- Often are structured as legally independent organizations
- Generally are not health plans, health care clearinghouses or health care providers, and therefore are *not* covered entities under HIPAA

See 45 CFR §164.502(e)(1)(ii)



HIEs (or RHIOs) Under HIPAA

- Structure has raised liability issues
- Generally operate through business associate agreements or memos of understanding

Minimum Necessary Rule & Treatment

- Applies to internal *uses* for treatment
 - A covered entity must have policies & procedures within an organization limiting access based on need for information
 - E.g., role based access to data


- Does *not* apply to *disclosures* to or requests by a health care provider for treatment

See 45 CFR § 164.502(b)



Minimum Necessary Rule & Treatment

- Many stakeholders still want to limit info. exchanged for treatment
 - Ethical guidelines
 - Fear of information overload
- Some use summary care documents (continuity of care record or document)
- Some use hospital discharge summaries



Minimum Necessary Rule & Payment

- Minimum necessary rule applies for using and disclosing health information for payment activities.
- HIE needs to ensure that requests/responses for data are limited to minimum amount necessary.

Disclosure of Information for HCO of Others


No individual permission required to disclose to another covered entity for the recipient's health care operations activities *only* if:

- Both entities had/have a relationship with the individual *and*
- For quality assessment and improvement, fraud detection, case management and specified other operations



Limited Data Set

- Considered protected health information
- Partially de-identified: Can include town or city, zip code, state, dates (e.g., date of birth) coded information
- Can disclose without individual authorization only for health care operations, research and public health purposes
- Requires a data use agreement



When Is Individual Permission (Consent) Required To Disclose Health Information?

- HIPAA does not preempt more stringent privacy standards
- These include laws that require consent to disclose information that HIPAA would allow to be shared without the individual's consent or authorization

42 CFR Part 2

- Not superseded by HIPAA
- Apply to alcohol and drug abuse patient records maintained by federally assisted alcohol and drug abuse program
- Require prior written consent to disclose even for treatment (except in emergency)

42 CFR Part 2

- Restriction doesn't apply to disclosures to a qualified service organization
- QSO includes
 - Entities that provide services to a program, such as data processing and bill collecting
- SAMHSA reviewing issue of QSOs and HIE



Non-Medicaid State Laws

May require individual permission before disclosing health information

- General health information confidentiality statutes and regulations
- Mental health laws
- HIV/AIDS laws



Some Approaches

- General opt in to participating in HIE to fulfill state requirements for general consent to share
- Condition-specific opt in to share sensitive information within the HIE




Some Approaches

- “When in doubt, leave it out.”
 - Vicki Estrin, TennCare
 - MA-Share Meds-Info –ED
- Incremental approach
 - Exchange general health information
 - Develop trust
 - Tackle tougher issues involving more “sensitive” health information



Future Approaches?

- Electronic consents
- Electronic systems to manage consents



PART 2
HIE and Information Security
for Medicaid/SCHIP Agencies

Walter G. Suarez, MD, MPH
President and CEO
Institute for HIPAA/HIT Education
and Research

Defining Health Information Exchange (HIE)

“The movement of health-related data—clinical and/or administrative –according to an agreed-upon set of interoperable standards, processes and activities across independently operating organizations in a manner that protects the privacy and security of an individual’s information.”

Source: “Consensus Conventions for the Use of Key HIT Terms” Project – ONC/HHS, 2008

RHIO and HIE – Distinguishing and Common Characteristics

RHIO

Entity that governs the interoperable exchange of health information

Entity that defines and has the authority & responsibility for establishing and enforcing information sharing policies and procedures

Exchanges clinical information and can exchange administrative information

Participants are geographically defined

Mission is to improve quality, safety, efficiency of healthcare for communities in which it operates

HIE

Activity or process that moves health-related data

Operates with an agreed upon set of interoperable standards, processes and activities needed to implement information exchange

Exchanges clinical or administrative information

Participants may be geographically defined or be non-geographic communities of affiliation

Purpose is to exchange information

Exchanges information among organizations that operate independently of each other



Exchanges information among organizations that operate independently of each other



Health Information Security and HIEs

- Security continues to be a critical aspect of creating and operating HIEs
- HIPAA Security provides a framework for establishing *internal* security policies and procedures
 - HIPAA Security does not provide a framework for secure HIEs
 - HIPAA Security does provide foundational components for entities to participate in HIEs



Health Information Security and HIEs

- HIEs present a number of security issues and challenges unique to the “external” aspect of information exchanges
 - Interoperability of Security Systems
 - Risk and Liability
 - Trust



Health Information Security and HIEs

- Interoperability of Security Systems
 - “Is my user identification compatible with your user identification?”
 - “Does my authentication ‘standard’ work with your authentication ‘standard’?”
 - “Do we have comparable access control policies?”



Health Information Security and HIEs

■ Risk and Liability

- “What are my additional risks and liabilities when connecting/exchanging data via an HIE?”
- “What is my liability if there is a security breach of the data I disclosed via an HIE?”

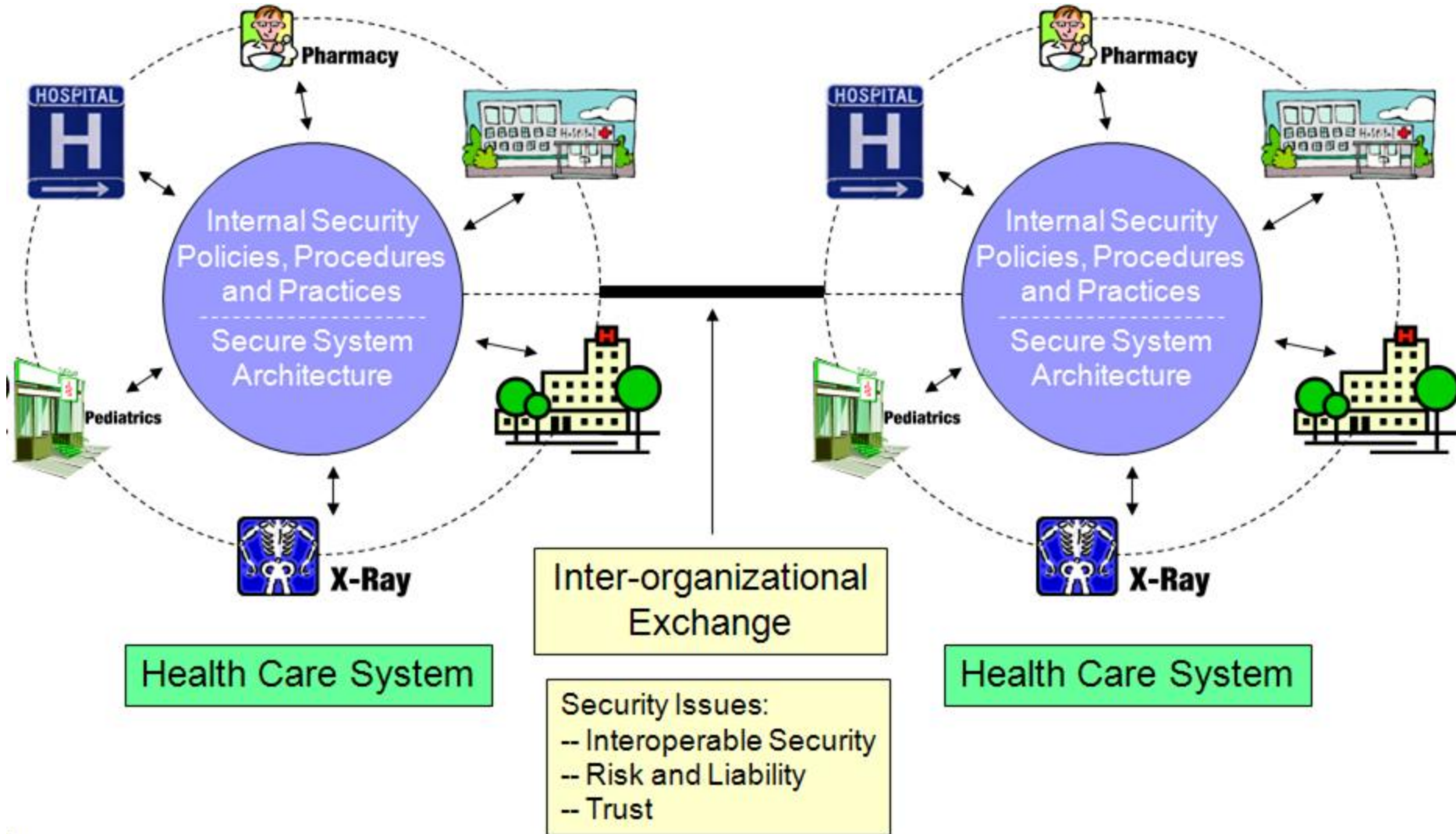


Health Information Security and HIEs

■ Trust

- “What is the minimum level of trust I should expect in an HIE agreement?”
- “How will multiple chain of trust agreements work in an HIE environment?”

Health Information Security and HIEs





Information Security - Core Concepts

- Overall goal: to safeguard the confidentiality, integrity and availability of information and systems
 - **Confidentiality** – ensuring that information and processing capability are protected from unauthorized disclosure or use
 - **Integrity** – ensuring that information held on information systems is not subject to malicious or accidental alteration and that system processes function correctly and reliably
 - **Availability** – ensuring that information systems, including stored information and processing capability, are always available to authorized users when needed



Information Security - Core Concepts

- The five cornerstones of information security
 - **Security Policies and Procedures** – establishing, implementing and maintaining internal policies, procedures, practices, guidelines and standards
 - **Security Architecture** – establishing, implementing and maintaining technical and system applications, hardware and related technologies to support the secure collection, storage, use and disclosure of information
 - **Assessment and Audit** – establishing mechanisms to ensure that security risks are assessed and identified, appropriate protections are in place



Information Security - Core Concepts

- The five cornerstones of information security (cont.)
 - **Accountability and Oversight** – establishing and assigning security responsibilities and monitoring compliance with security policies and procedures
 - **Training and Awareness** – ensuring that staff are aware of the importance of security and empowering staff with skills needed to conduct their work



*Information Security and
Medicaid/SCHIP Participation
in HIEs*



Key Security Factors Affecting Medicaid/SCHIP Participation in HIEs

- Policy References (Federal and State Laws and Regulations)
- MMIS/MITA Architecture
- Availability of Interoperable Security (and Privacy) Standards for HIE
- HIE Agreements, Risk and Liability Issues



Security Policy References

- Federal Laws and Regulations
 - HIPAA Security requirements established a base level of security for protecting internal information resources
 - Scalability, flexibility and ‘reasonable and appropriate’ provisions allow for multiple internal security approaches to be used
 - No federal regulation establishing security requirements for HIEs

Security Policy References

- State Laws and Regulations
 - States have established laws requiring adoption and use of security standards and practices
 - Applicable to all industries
 - Applicable to government systems
 - Applicable to health care industry
 - Addressing specific security issues (i.e. breaches)
- Medicaid/SCHIP Program Requirements
 - Program requirements (reflecting federal and/or state regulations) further limit sharing of information with others



*MMIS/MITA Architecture
and Security*



MMIS/MITA Architecture and Security

- Technical principles of MITA include:
 - Security and privacy must be integrated throughout the architecture
 - Model architecture ensures interoperability within the various system components
 - Interoperability standards are to be established and followed
 - Secure data exchange is to be supported and promoted



MITA Security Principles

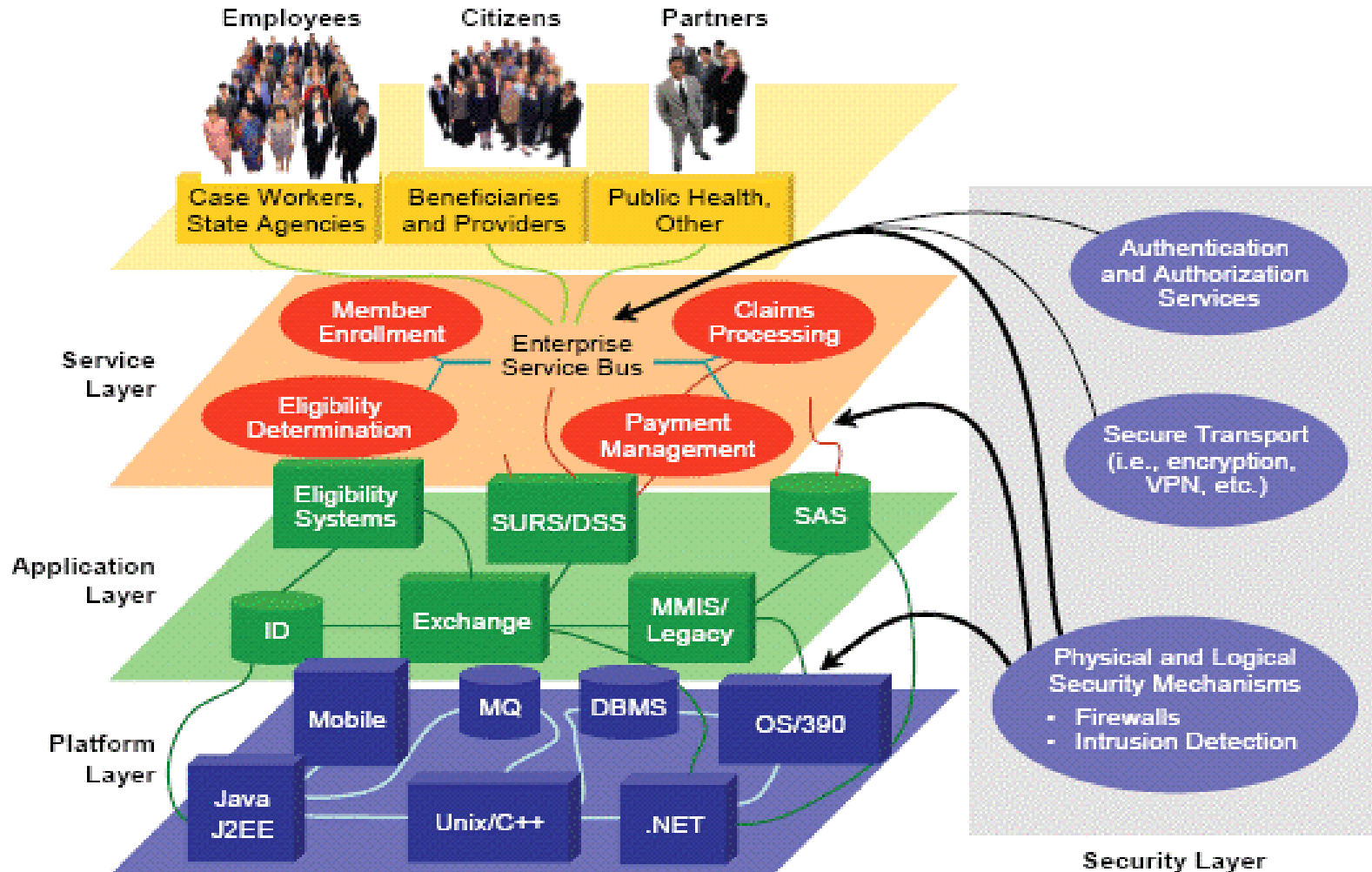
- **Compartmentalize** – reduce the ‘surface area’ of attack (i.e. use of firewalls)
- **Use Least Privilege** – run processes using accounts with minimal privileges and access rights
- **Apply Defense in Depth** – use multiple gatekeepers to keep attackers at bay (not relying on a single layer of security)
- **Do Not Trust User Input** – assume that all input is malicious until proved otherwise (ensure input validation)
- **Check at the Gate** – authenticate and authorize users early – at first gate



MITA Security Principles (cont.)

- **Fail Securely** – ensure that sensitive data is not left accessible if a system component/application fails
- **Secure Weakest Link** – identify any vulnerabilities in the network that an attacker can exploit
- **Create Secure Defaults** – set-up the default account with least privileges, disable default account and only enable it when needed, etc
- **Reduce Attack Surface** – disable or remove unused services, protocols and functionality

MMIS/MITA Architecture and Security





*Availability of Interoperable Security
(and Privacy) Standards for HIEs*

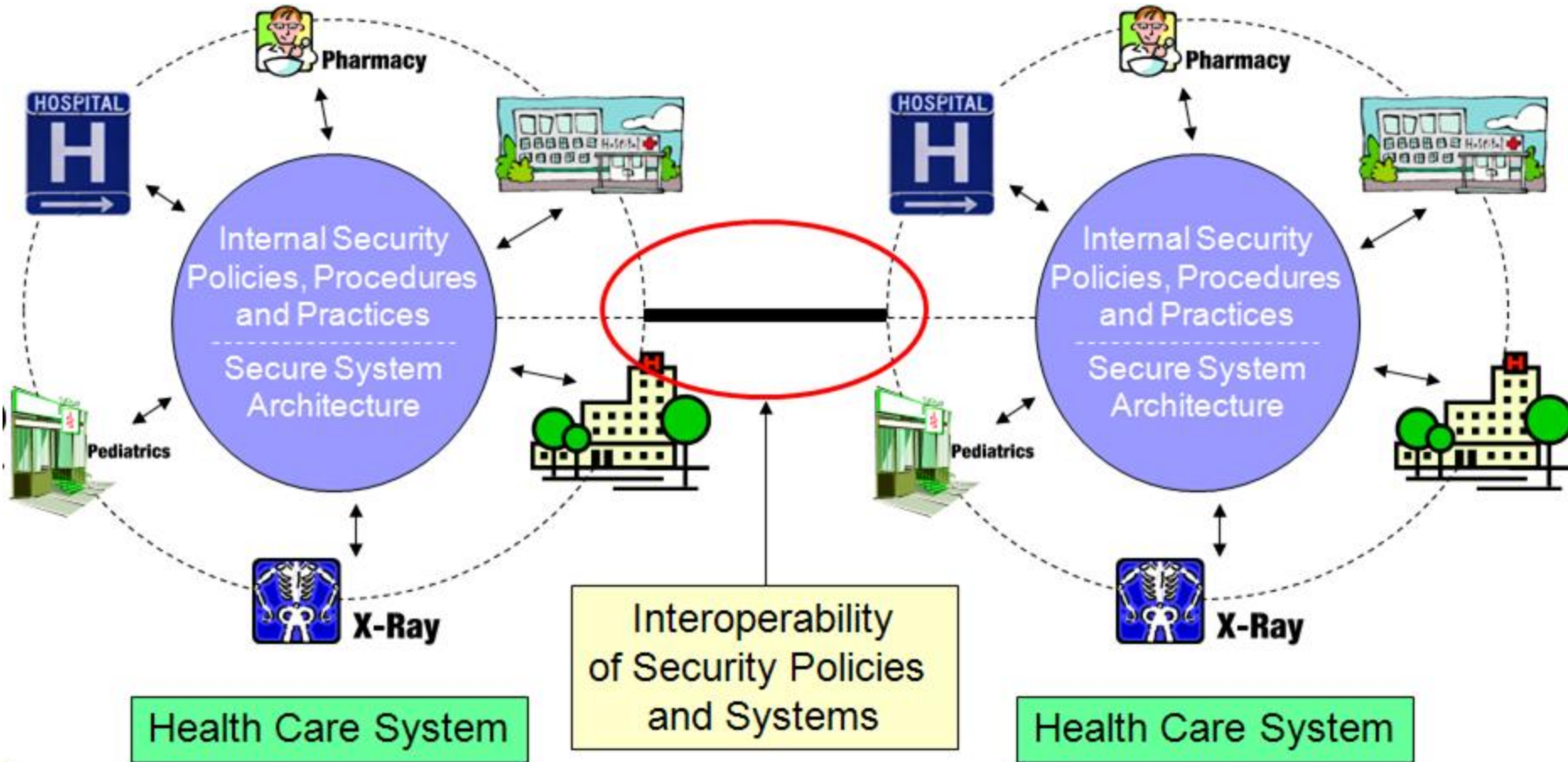


What is “Interoperability”

“The ability of different information technology systems and software applications to communicate, to exchange data accurately, effectively and consistently, and to use the information that has been exchanged.”

Source: National Alliance for Health Information Technology, July 2005; “Consensus Conventions for the Use of Key HIT Terms” Project – ONC/HHS, 2008

Health Information Security and HIEs



Interoperable Security Requirements

- **Accountability Controls** – The controls that can prove the system is protecting the resources in accordance to policies. They include security audit logging, reporting, alerting and alarming
- **Identification and Authentication Controls** – The controls that prove that a system or person is who they say they are. For example, personal interactions, digital certificates, security assertions.
- **Access Controls** – The controls that limit access by an authenticated entity to the information and functions that they are authorized to have access to. Often implemented using Role Based Access Controls (RBAC)

Interoperable Security Requirements (cont.)

- **Confidentiality Controls** – As sensitive information is created, stored, communicated, and modified, this control protects the information from being exposed. For example, encryption.
- **Data Integrity Controls** –The controls that prove that the data has not changed in an unauthorized way. For example: digital signatures, secure hash algorithms, CRC, and checksum.
- **Non-Repudiation Controls** – The controls that ensure that an entity can not later refute that they participated in an act. For example: author of a document, order of a test, prescribe of a prescription.



Interoperable Security Requirements (cont.)

- **Patient Privacy Controls** – The controls that enforce patient specific consent directive instructions.
- **Availability Controls** – The controls that ensure that information is available when needed. For example: backup, replication, fault tolerance, RAID, trusted recovery, uninterruptible power supplies, etc.

Health Information Technology Standards Panel (HITSP)



The Panel's Purpose

To harmonize and integrate diverse **standards** that will meet clinical and business needs for sharing information among organizations and systems.

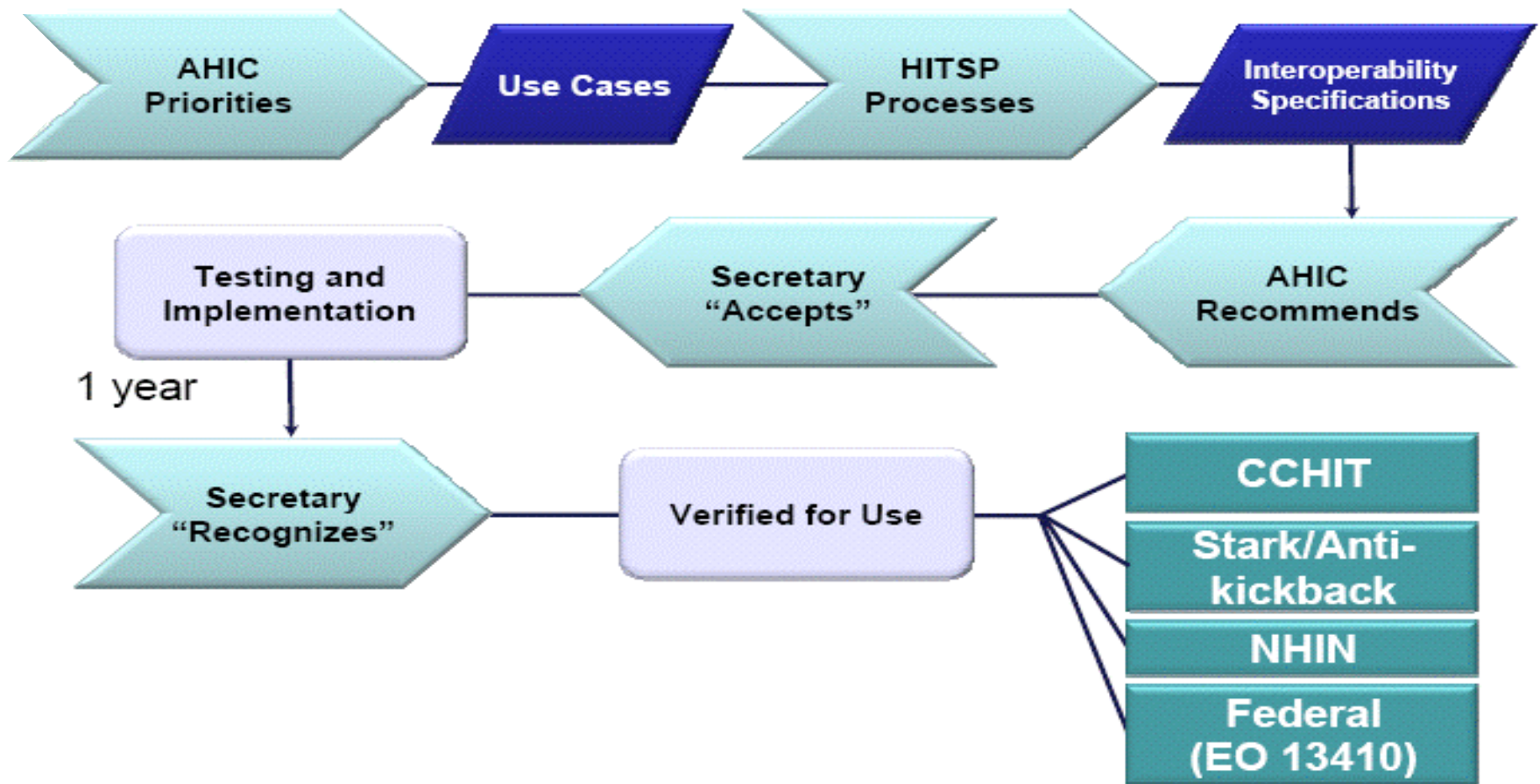
- Establish HITSP Interoperability Specifications and promote their acceptance;
- Support the deployment and implementation of HITSP Interoperability Specifications across the health care enterprise;
- Facilitate the efforts of standards developing organizations to maintain, revise or develop new standards as required to support the HITSP Interoperability Specifications.

Harmonized standards promote interoperability, enhance healthcare quality and contain costs



Health Information Technology Standards Panel (HITSP)

Standards Acceptance Process



HITSP Final Recognized Privacy and Security Constructs

- **Secured Communication Channel (HITSP T17)**
 - A mechanism to ensure the authenticity, integrity and confidentiality of the transaction
 - Provides mutual node authentication, transmission integrity and transmission confidentiality
 - Uses IHE ATNA Profile
- **Consistent Time (HITSP T16)**
 - A mechanism to ensure that the system clocks and time stamps of the network computers are synchronized
 - Uses IHE Consistent Time Profile
- **Non-Repudiation of Origin (HITSP C26)**
 - A mechanism to ensure proof of origin of a document
 - Uses IHE DSG Profile

HITSP Final Recognized Privacy and Security Constructs (cont.)

- **Manage Sharing of Documents (HITSP TP13)**
 - A mechanism to ensure the integrity of a document being shared
 - Uses ISO 15000 ebRS, IHE XDS and IHE NAV
- **Entity Identity Assertion (HITSP C19)**
 - A mechanism to correctly authenticate the identity of a user
 - Uses OASIS SAML 2.0 and WS-Security
- **Manage Consent Directives (HITSP TP30)**
 - A mechanism to record consent directives electronically
 - Uses “Basic Patient Privacy Consent” profile from IHE
 - Uses HL7 consent code standards and confidentiality codes

HITSP Final Recognized Privacy and Security Constructs (cont.)

■ **Access Control (HITSP TP20)**

- A mechanism to determine if access to system resources and functions are to be authorized
- Uses a combination of privacy policies, security policies and enforcement of the resulting merged set of policies
- Uses WS-Federation, WS-Trust, OASIS SAML and XACML

■ **Collect/Communicate Security Audit Trail (HITSP T15)**

- A mechanism to provide assurance that security policies are being followed/enforced and that risks are being mitigated
- Uses the IHE ATNA Profile



Summary – Security and HIEs

- Interoperability of security systems continues to be a key factor in the deployment of HIEs
- HIPAA Security has provided a good foundation for Medicaid and SCHIP participation in HIEs
- Remaining policy and legal limitations will need to be addressed, for Medicaid/SCHIP agencies to participate in an HIE
- Medicaid/SCHIP systems (MMIS/MITA) will need to be capable of supporting HITSP interoperable security and privacy constructs
- Medicaid/SCHIP should become more engaged in HITSP interoperability efforts



Project Information

Please send comments and recommendations to:
Medicaid-SCHIP-HIT@ahrq.hhs.gov

or Call Toll-free:

1-866-253-1627

Medicaid-SCHIP-HIT@ahrq.hhs.gov
<http://healthit.ahrq.gov>