

# HITSP Security and Privacy

Johnathan Coleman, CISM, CISSP  
Principal, Security Risk Solutions, Inc.  
HITSP Security and Privacy Technical Committee Facilitator



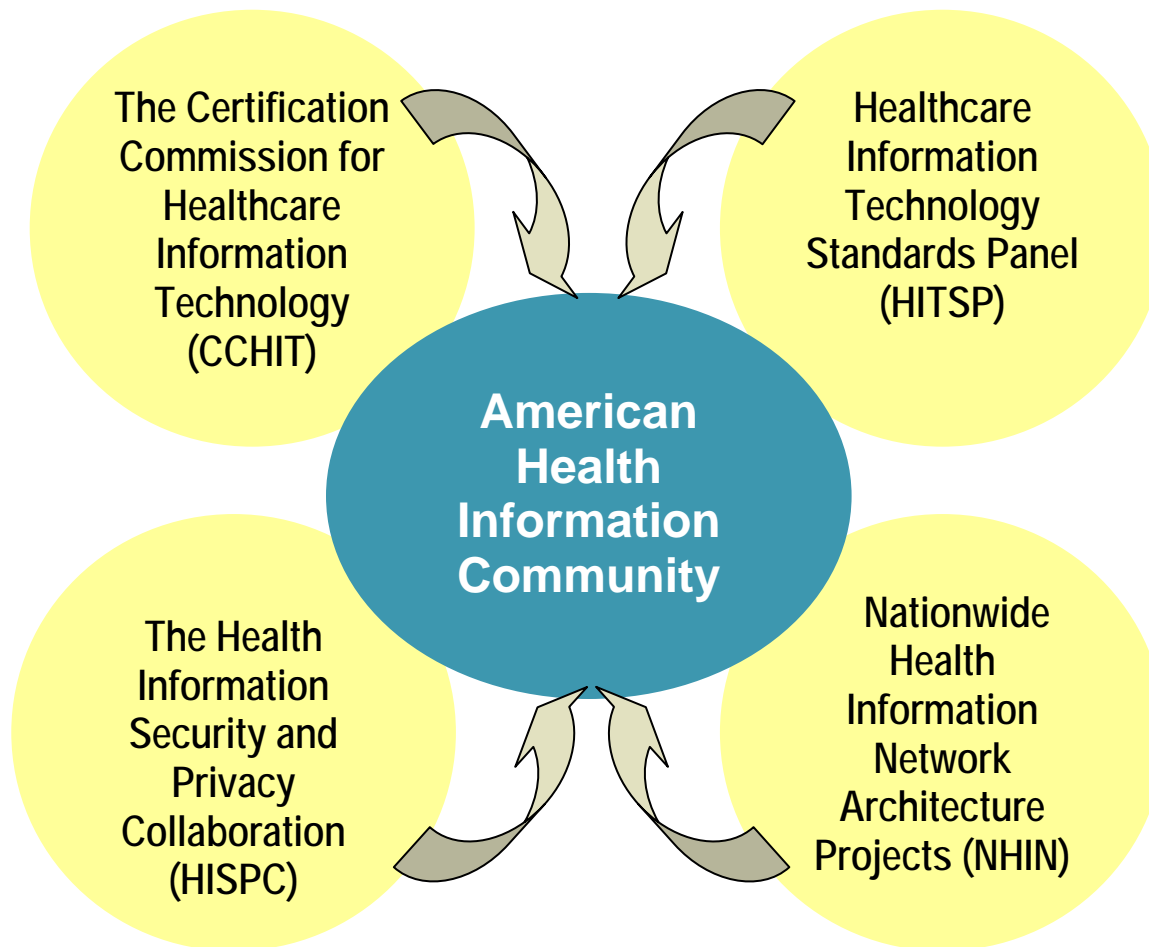
April 25, 2007

# Agenda

1. Relationship between HITSP, HISPC and CCHIT
2. HITSP Charter and Goals
3. Harmonization Process
4. Current Status of HITSP Security and Privacy Activities
5. HITSP Security and Privacy Constructs under Consideration
6. HITSP Contact Information



# A public-private “Community” was established to serve as the focal point for America’s health information concerns and drive opportunities for increasing interoperability



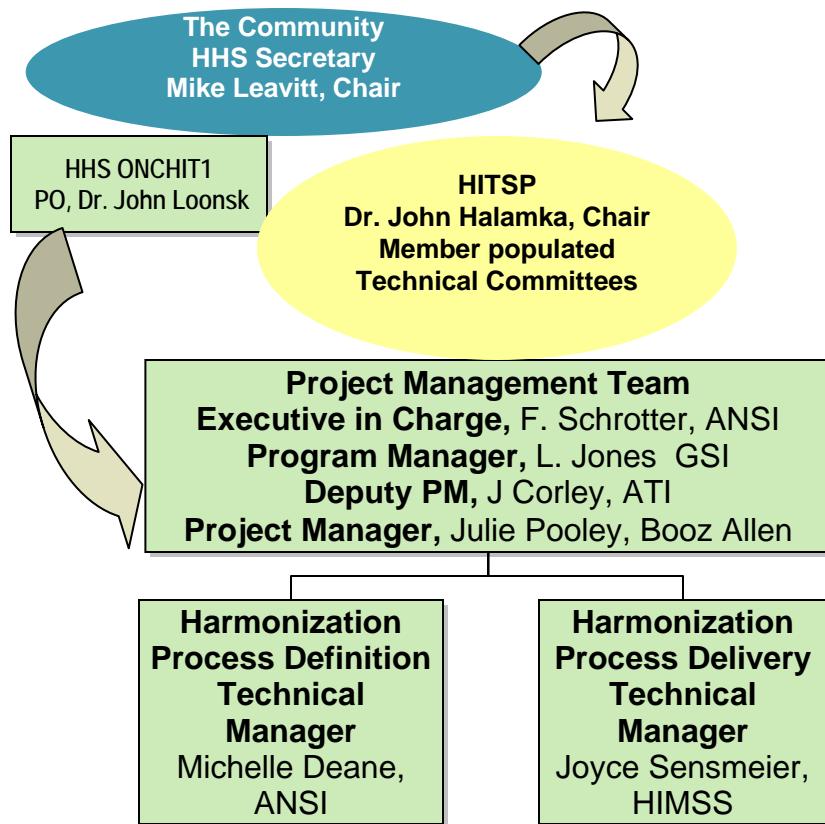
*HITSP includes 348 different member organizations and is administered by a Board of Directors*

- 24 SDOs (7%)
- 247 Non-SDOs (71%)
- 30 Govt. bodies (9%)
- 12 Consumer groups (3%)
- 36 Project Team and Undeclared (10%)

*The Community is a federally-chartered commission and will provide input and recommendations to HHS on how to make health records digital and interoperable, and assure that the privacy and security of those records are protected, in a smooth, market-led way.*



# The HITSP team is charged with completing eleven different tasks, with current efforts focused on the harmonization process



Eleven Tasks are included in this contract:

1. Comprehensive Work Plan
2. Conduct a Project Start Up Meeting
3. Deliver Recommended Use-Cases
4. Participate in related meetings and activities, including the AHIC Meetings
5. Develop a Gap Analysis
6. Standards Selection, Evaluations and Testing
7. Define a Harmonization Approach
8. Develop Interoperability Specifications
9. Develop and Evaluate a Business Plan for the self-sustaining processes
10. Submit Monthly Reports – ongoing efforts
11. Assist with communications – ongoing efforts



## HITSP formed Technical Committees to focus on AHIC breakthrough areas - Initial focus is on 3 use cases

- ▶ **Biosurveillance** -- Transmit essential ambulatory care and emergency department visit, utilization, and lab result data from electronically enabled health care delivery and public health systems in standardized and anonymized format to authorized public health agencies with less than one day lag time.
- ▶ **Consumer Empowerment** -- Deploy to targeted populations a pre-populated, consumer-directed and secure electronic registration summary. Deploy a widely available pre-populated medication history linked to the registration summary.
- ▶ **Electronic Health Records** -- Deploy standardized, widely available, secure solutions for accessing laboratory results and interpretations in a patient-centric manner for clinical care by authorized parties.
- ▶ **Security and Privacy** – Initially a formed as a Work Group to address Security and Privacy (S & P) requirements of the first three Use Cases. Now a Technical Committee charged with addressing S & P requirements for all Use Cases provided to HITSP.



## HITSP Coordinating Committees and Leadership

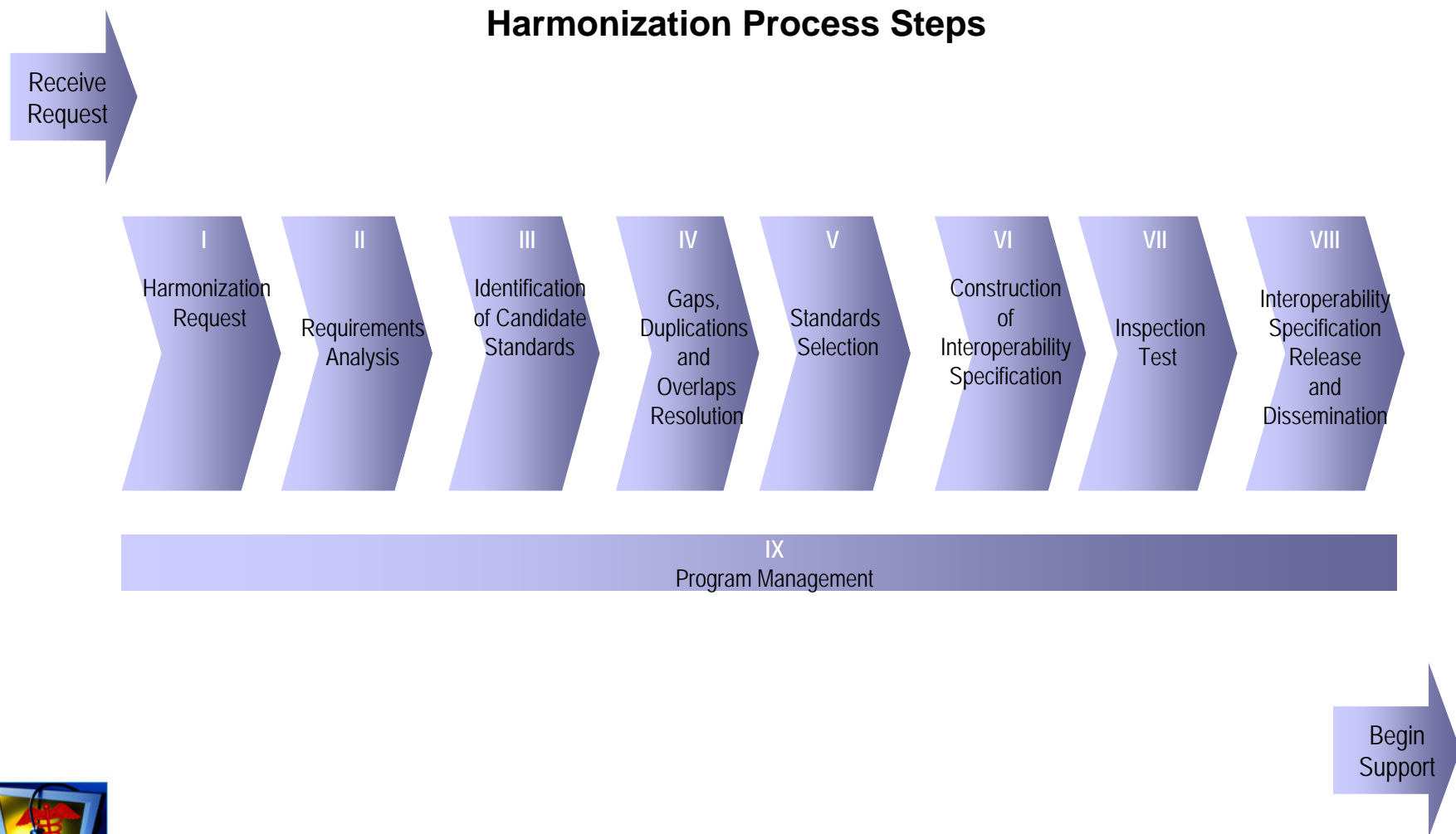
- ▶ **Foundations Committee**
  - Steve Wagner
  - Bob Dolin
- ▶ **HITSP Process Review Committee**
  - Lynne Gilbertson
  - Erik Pupo
- ▶ **HITSP-CCHIT Joint Work Group**
  - Jamie Ferguson, Kaiser Permanente
- ▶ **Harmonization Readiness Committee**
  - Lynne Gilbertson
- ▶ **Business Plan Committee**
  - Steve Lieber
- ▶ **International Landscape Committee**
  - Bill Braithwaite
- ▶ **Governance Committee**
  - Michael Aisenberg

## HITSP Technical Committees and Leadership

- ▶ **HITSP Technical Committee - Care Delivery**
  - James Ferguson, Kaiser Permanente
  - Steve Hufnagel, DoD
  - Steve Wagner, Department of Veterans Affairs
- ▶ **HITSP Technical Committee - Consumer Empowerment**
  - Elaine Blechman, PhD, University of Colorado, Boulder
  - Charles Parisot, GE Healthcare
  - Scott Robertson, Kaiser Permanente
- ▶ **HITSP Technical Committee- Population Health**
  - Floyd Eisenberg, MD, MPH, Siemens Medical Solutions
  - Peter Elkin, MD, Mayo Clinic College of Medicine
  - Shaun Grannis, Department of Family Medicine, Indiana University School of Medicine
- ▶ **HITSP Technical Committee- Security and Privacy**
  - Cochair nominations in progress



# The actual harmonization process is a series of steps taken by industry stakeholders within the context of HITSP



## HITSP Security and Privacy Goals/Charter

- ▶ Harmonize HITSP standards for EHR-Lab reporting, Population Health and Consumer Empowerment with relevant Security and Privacy standards.
- ▶ Convene regular meetings with adequate representation from each TC to review current Interoperability Specifications and identify areas of Security and Privacy that were previously deferred.
  - This will be expanded to include Security and Privacy requirements from the ER-EHR Use Case and other new Use Cases provided to HITSP
- ▶ Begin work on identifying security standards, approaches, and identifying unresolved issues. Leverage activities of other Security and Privacy related workgroups.
  - The purpose of the HITSP TC is to ensure that technical standards to address privacy and security needs are identified and harmonized. We will rely on both the HISPC project and the State Alliance for e-Health to inform our work surrounding policy and regulatory considerations.

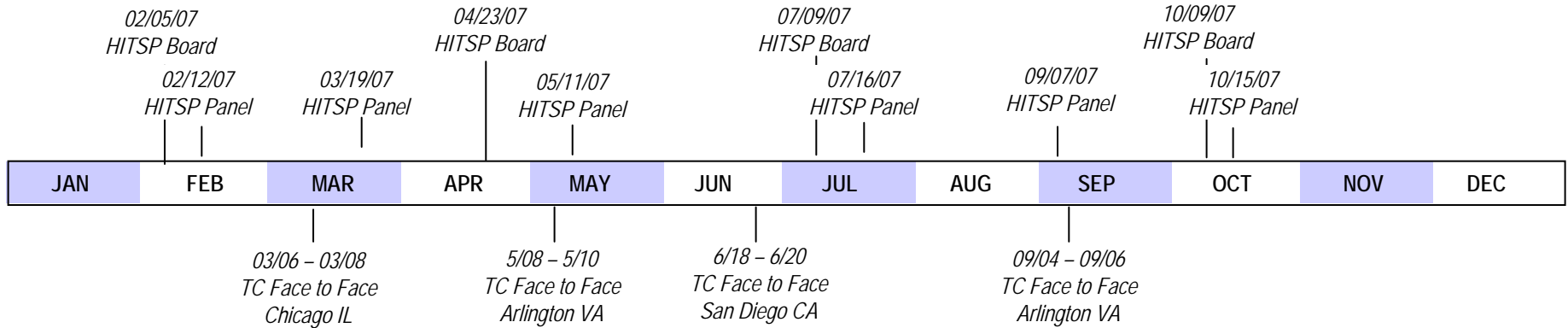


## Current Status of HITSP Security and Privacy Activities

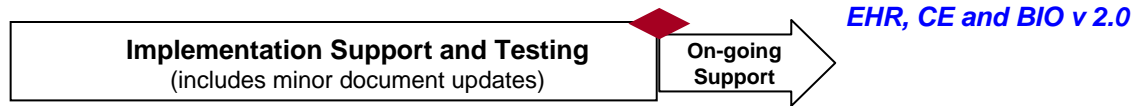
- ▶ Review Use Cases and identify Security and Privacy Requirements. This will serve to populate the Requirements sections of the Requirements, Design and Standards Selection (RDSS) document. **Completed**
- ▶ Identify *candidate* standards (from our Inventory of Standards and other sources), and sort them into buckets which correspond to the security and privacy requirements (potential HITSP constructs). **Completed**
- ▶ Develop Requirements, Design, Standards Selection (RDSS) document **Completed**
  - Technical Actors, Business Actors & mappings from use cases
  - UML diagrams (initially a high level relationship roadmap)
  - Identify Security and Privacy Requirements and map to use cases
  - **Public Comment Period: 05/16 – 06/14**
- ▶ Apply Tier 2 criteria to *select* from the existing standards for each of our potential constructs. **Current Activity**
- ▶ Develop HITSP Security and Privacy Constructs which will frame implementation of the selected standards to achieve the requirements as identified in the Use Cases. **Current Activity**
- ▶ Inspection Test and Public Comment: **07/20 – 08/16**
- ▶ Comment Resolution and Panel Approval: **08/17 – 10/15**



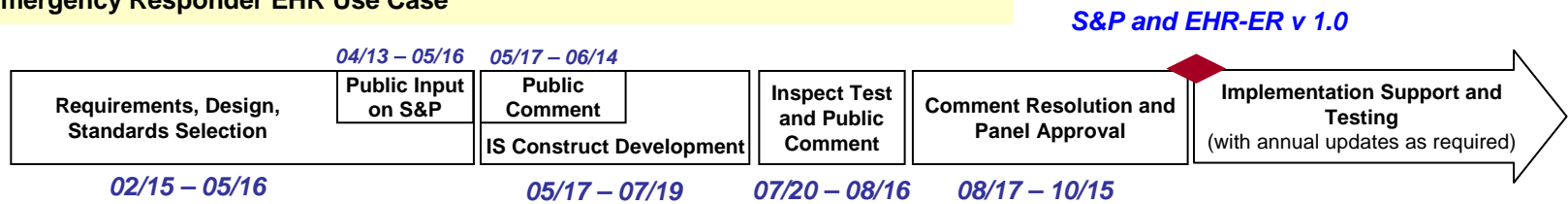
# HITSP 2007 Timeline



## Activity 1 – Version 2.0 of Existing EHR, CE, BIO ISs



## Activity 2 – Security and Privacy for All Use Cases Activity 3 – New Emergency Responder EHR Use Case



## Activity 4 –New Use Cases from AHIC



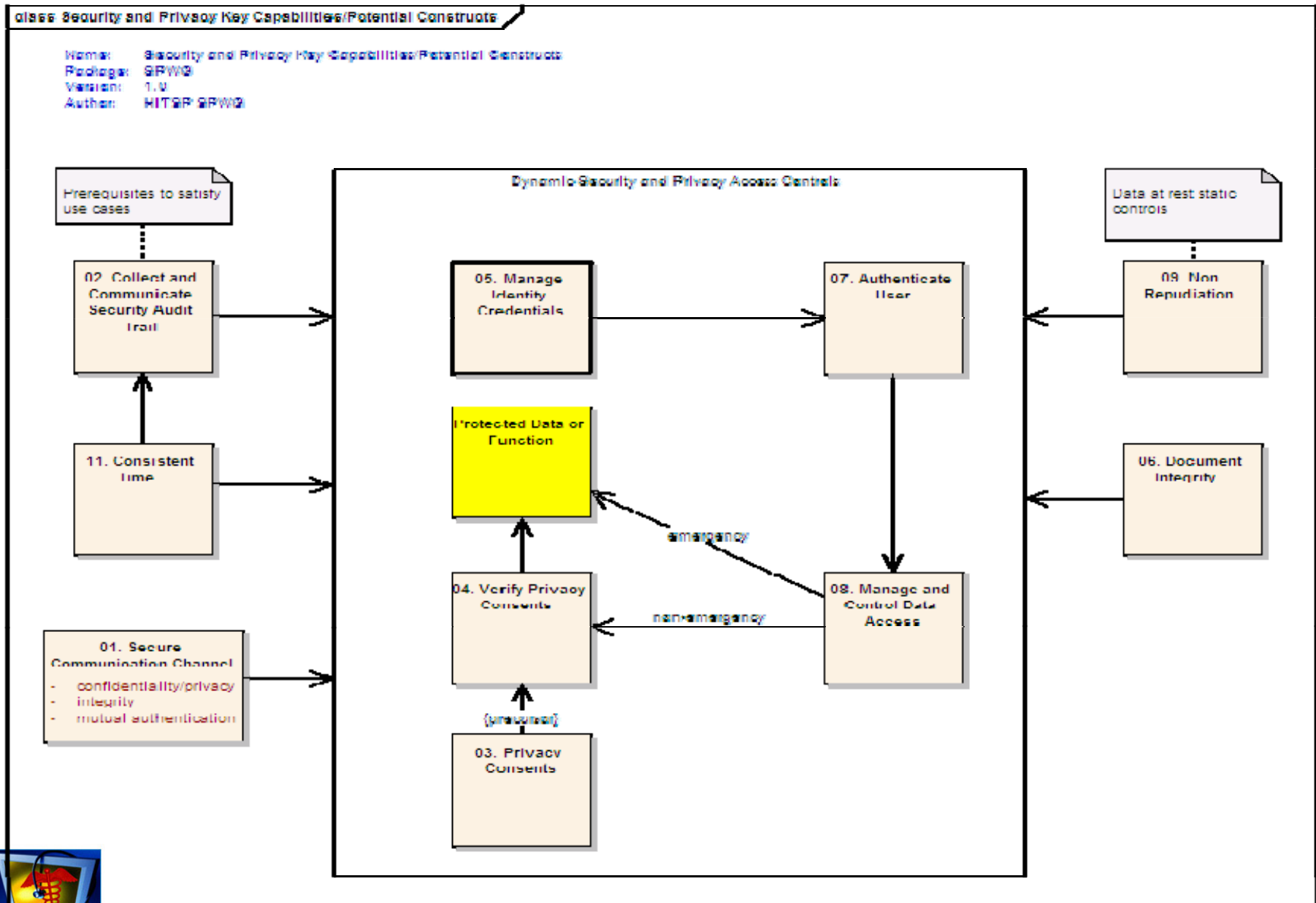
Evaluation of Standards Harmonization Process for HIT

# HITSP Security and Privacy Constructs under Consideration

1. Secured Communication Channel  
(includes mutual node authentication, integrity and confidentiality of transmission contents)
2. Collect and Communicate Security Audit Trail
3. Privacy Consents
4. Verify Privacy Consents
5. Manage Entity Identity Credentials
6. Document Integrity
7. Authenticate User
8. Manage and Control Data Access
9. Non Repudiation
10. Fail-Safe/Emergency access (now rolled into #4 and #8)
11. Consistent Time



# HITSP Security and Privacy Constructs under Consideration



## Questions

- ▶ For General Technical Committee related questions please contact:

Joyce Sensmeier MS, RN-BC, CPHIMS, FHIMSS  
Vice President, Informatics  
HIMSS  
230 East Ohio, Suite 500  
Chicago, IL 60611-3269  
Phone: 312-915-9281 email: [jsensmeier@himss.org](mailto:jsensmeier@himss.org)

Or

Jessica Kant  
Coordinator, Standards Harmonization  
Healthcare Information & Management Systems Society  
230 E. Ohio St., Suite 500  
Chicago, IL 60611  
Phone: 312-915-9283 Fax: 312-915-9511 email: [jkant@himss.org](mailto:jkant@himss.org)

- ▶ For HITSP Security and Privacy related questions please contact:

Johnathan Coleman  
Principal, Security Risk Solutions, Inc.  
690 Libbys Pt.  
Mt. Pleasant, SC 29464  
Tel: 843-442-9104 email: [jc@securityrisksolutions.com](mailto:jc@securityrisksolutions.com)



# Supplementary Slides

- ▶ The following slides to be used during discussions if necessary



## HITSP Definition of a Standard

- ▶ A standard specifies a well-defined approach that supports a business process and: (1) has been agreed upon by a group of experts; (2) has been publicly vetted; (3) provides rules, guidelines, or characteristics; (4) helps to ensure that materials, products, processes, and services are fit for their intended purpose; (5) is available in an accessible format; and (6) is subject to an ongoing review and revision process.



## Tier 2 Standards Readiness Criteria

- ▶ Suitability
  - The standard is named at a proper level of specificity and meets technical and business criteria of use case
- ▶ Compatibility
  - The standard shares common context, information exchange structures, content or data elements, security and processes with other HITSP harmonized standards or adopted frameworks as appropriate
- ▶ Preferred Standards Characteristics
  - Approved standards, widely used, readily available, technology neutral, supporting uniformity, demonstrating flexibility and international usage are preferred
- ▶ Standards Development Organization and Process
  - Meet selected criteria including balance, transparency, developer due process, stewardship and others.
- ▶ Total Costs and Ease of Implementation
  - Deferred to future work



## HITSP Technical Committees Terms of Reference

- ▶ Perform high level **Requirements Analysis and Design** of HITSP Interoperability Specifications, transaction packages, transactions, components, constructs including requirements analysis, and minimum data set.
- ▶ Identify, analyze and document **gaps and duplications** within the standards industry as they are related to each specific Use Case.
- ▶ Review and scope statements of work for each new use case.
- ▶ Provide a listing of all standards that satisfy the requirements imposed by the relevant use cases as well as **readiness criteria** that shall be used to evaluate the standard.
- ▶ **Select and evaluate recommended standards** to meet the relevant Use Case.
- ▶ Develop, review and evaluate '**interoperability specifications**' for the selected standards.
- ▶ Submit **recommendations to HITSP** for review, approval and resolution.
- ▶ Ensure timely response and **disposition** of comments.
- ▶ Ensure **on-going process** for addressing corrections/change requests and resolutions.



# HITSP Framework

## Basis for Interoperability Specification Template

- ▶ HITSP receives Use Cases and Harmonization Requests from external sources, such as AHIC and ONC.
- ▶ The Use Case or Request defines scenarios, business actors, and business and functional/interoperability requirements.
- ▶ HITSP decomposes the Use Case requirements into scenario(s) and then into transactions providing context: technical actors, actions and content. It may create or reuse a transaction or a grouping of transactions (transaction package) based on commonality at this level.
- ▶ Transactions are logical groupings of actions that are decomposed into components, which are groupings of base standards that work together, such as message and terminology.
- ▶ Each HITSP construct, i.e., transaction package, transaction or component, may constrain the construct or standard below it. Constraints follow a strict hierarchy and are only imposed by the next higher construct.
- ▶ Transaction packages, transactions and components all are potential candidates for reuse if a new set of requirements and context are successfully fulfilled by the existing construct.
- ▶ While reuse is a HITSP goal, it is established in the context of a Use Case and its functional/interoperability requirements.
- ▶ HITSP constructs are version controlled and, if reused, will be uniquely identified.



# Definitions and Rules

Level	Definition	Example	Rules
Use Case or Harmonization Request	<ul style="list-style-type: none"> <li>▪ Defines business/functional requirements</li> <li>▪ Sets Context</li> </ul>	<ul style="list-style-type: none"> <li>▪ ONC Harmonized EHR Use Case</li> </ul>	
Interoperability Specification	<ul style="list-style-type: none"> <li>▪ Models business/ functional/ interoperability requirements</li> <li>▪ Identifies technical/system requirements to meet use-case</li> <li>▪ Identifies how to use one or more HITSP constructs to meet use-case requirements</li> </ul>	<ul style="list-style-type: none"> <li>▪ HITSP EHR Interoperability Specification</li> </ul>	<ul style="list-style-type: none"> <li>▪ Based on UML diagram to identify technical actors and actions</li> <li>▪ Sets context</li> <li>▪ Testable functional requirements</li> <li>▪ Ids transactions or transaction packages</li> </ul>
Transaction Package	<ul style="list-style-type: none"> <li>▪ Defines how two or more transactions are used to support a stand-alone information interchange within a defined context between two or more systems</li> </ul>	<ul style="list-style-type: none"> <li>▪ Record Locator Service</li> <li>▪ Entity Identification Service</li> </ul>	<ul style="list-style-type: none"> <li>▪ Thin context and interoperability requirements</li> <li>▪ Testable</li> <li>▪ Based on analysis of like technical actors, context and content harmonized across transactions</li> <li>▪ May be fulfilled by one or more transactions or composite standard</li> <li>▪ Expresses constraints on the transactions or composite standard</li> </ul>
Transaction	<ul style="list-style-type: none"> <li>▪ Logical grouping of actions, including necessary content and context, that must all succeed or fail as a group.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Query lab result</li> <li>▪ Send lab result</li> </ul>	<ul style="list-style-type: none"> <li>▪ Fulfills all actions between two or more systems needed to meet one or more interoperability requirements</li> <li>▪ Testable</li> <li>▪ May be fulfilled by components or composite standard</li> <li>▪ Expresses constraints on components or composite standard</li> </ul>



## Definitions and Rules (cont.)

Level	Definition	Example	Rules
Component	<ul style="list-style-type: none"> <li>An atomic construct used to support an information interchange or to meet an infrastructure requirement (e.g., security, logging/audit)</li> </ul>	<ul style="list-style-type: none"> <li>Lab result message</li> <li>Lab result context</li> </ul>	<ul style="list-style-type: none"> <li>Typically will use one “primary” standard and may have other “secondary” standards</li> <li>Expresses constraints on base or composite standards</li> </ul>
Base Standard	<ul style="list-style-type: none"> <li>A standard capable of fulfilling a discrete function within a single category produced and maintained by a single standards organization.</li> </ul>	<ul style="list-style-type: none"> <li>Messaging standard</li> <li>Security standard</li> <li>Code set.</li> </ul>	<p>Per HITSP definition the term “standard” refers, but is not limited to,:</p> <ul style="list-style-type: none"> <li>– Specifications</li> <li>– Implementation Guides</li> <li>– Code Sets</li> <li>– Terminologies</li> <li>– Integration Profiles</li> </ul>
Composite Standard	<ul style="list-style-type: none"> <li>Grouping of coordinated base standards, often from multiple standards organizations, maintained by a single organization. In HITSP, it can serve as a component, transaction or transaction package functional requirements..</li> </ul>	<ul style="list-style-type: none"> <li>Integration profiles</li> <li>Implementation guides</li> <li>Health transaction services</li> </ul>	Per Definition above



**Candidate Standards with Potential Applicability to the Application of Consents**

IS22857	Health informatics -- Guidelines on data protection to facilitate trans-border flows of personal health information
IS17090 part1,2,3	Health informatics -- Public key infrastructure
TS26000 part1,2	Health informatics - Privilege management and Access Control
IS27799	Health informatics: Security management in health using IS17799
DTS21298	Health informatics: Functional and Structural Roles
prEN_13606-4	Health informatics — Electronic health record communication — Part 4: Security requirements and distribution rules
E1869	Standard Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Electronic Health Records
E1985	Standard Guide for User Authentication and Authorization
E1986	Standard Guide for Information Access Privileges to Health Information
E1987	Standard Guide for Individual Rights Regarding Health Information
XACML	eXtensible Access Control Markup Language (XACML)
SAML	Security Assertion Markup Language (SAML)
LDAP	Lightweight Directory Access Protocol
X.500	The CCITT and ISO standard for electronic directory services
RFC 3280	Internet X.509 Public Key Infrastructure Certificate and CRL Profile
RFC 2560	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
RFC 2259	Internet X.509 Public Key Infrastructure Operational Protocols—LDAPv2
RFC 2560	Internet X.509 Public Key Infrastructure Online Certificate Status Protocol
RFC 3852	Cryptographic Message Syntax (CMS).
ISO 9594-1,2	Information technology -- Open Systems Interconnection -- The Directory
ISO 9796-2,1	Information technology -- Security techniques -- Digital signature schemes giving message recovery
ITU-T X.501	Information Technology Open Systems Interconnection—The Directory: Models
PKCS #8:	Private-Key Information Syntax Standard
DSG	Document Digital Signature
BPPC	Patient Consent
HL7 v3 RBAC vocabulary	V3 Role based access control
HL7 EHR-S	EHR functional Criteria: Conformance Criteria
HL7 v3	Medical records: consent topic

