

# Healthcare Information Technology Standards Panel

Johnathan Coleman, *CISSP, CISM*  
*jc@SecurityRiskSolutions.com*

**Facilitator, HITSP Security and Privacy Technical Committee**



# HITSP Membership

---

- ▶ **A total of 379 organizations participating in HITSP representing a broad spectrum of interests:**
  - Standards Development Organizations (24)
  - Non-SDOs such as clinicians, providers, safety net providers, vendors, purchasers, payers, public health professionals, and researchers (308)
  - Government organizations (32)
  - Consumer organizations (15)
  - (+Plus 89 informational organizations)



# Technical Committees

---

- ▶ **Total Technical Committee Membership – 391 individuals**
- ▶ **Attendance at face to face meetings averages 100 individuals**
- ▶ **Numerous weekly teleconferences**
- ▶ **Incredible amounts of off-line work by sub-groups and individuals**
- ▶ **Sponsor harmonization and joint development efforts with standards organizations**



# HITSP Interoperability Specification Catalog

---

- ▶ IS01 - Electronic Health Records Laboratory Results Reporting
- ▶ IS02 - Biosurveillance
- ▶ IS03 - Consumer Empowerment and Access to Clinical Information via Networks
- ▶ IS04 - Emergency Responder Electronic Health Record
- ▶ IS05 - Consumer Empowerment and Access to Clinical Information via Media
- ▶ IS06 - Quality
- ▶ IS07 - Medication Management



# TN900 – Security and Privacy Technical Note

---

- ▶ Provides implementation guidance to address Security and Privacy requirements of the AHIC Use Cases
  - Collect and Communicate Security Audit Trail
  - Consistent Time
  - Secured Communication Channel
  - Entity Identity Assertion
  - Access Control
  - Non-repudiation of Origin
  - Manage Consent Directives
  - Manage Sharing of Documents
  
- ▶ Provides a broad framework to support a variety of methodologies and approaches
  
- ▶ Will continue to be reused for future Use Cases



# HITSP Security and Privacy Constructs

---

- ***Identification of Core Set of Constructs*** -- A core set of Privacy and Security constructs identified from all use cases; constructs reviewed and validated/modified upon receipt of new use cases
- ***Incorporation of Constructs into Other Technical Committee Documents*** – Privacy and security constructs are incorporated into the documents created by the other TCs to address interoperability in their respective use cases



# HITSP Security and Privacy Constructs

Construct Name	HITSP Reference	Type of Construct	Definition
Manage Sharing of Documents (with Document Integrity inserted as an option)	HITSP/TP13	Transaction Package	To ensure the integrity of a document that is exchanged or shared
Collect and Communicate Security Audit Trail	HITSP/T15	Transaction	To define and identify security relevant events and the data to be collected and communicated as determined by policy, regulation, or risk analysis
Consistent Time	HITSP/T16	Transaction	To ensure that all the entity systems that are communicating within the network have synchronized system clocks
Secured Communication Channel	HITSP/T17	Transaction	To ensure the authenticity, the integrity, and the confidentiality of Transactions, and the mutual trust between communicating parties
Entity Identity Assertion	HITSP/C19	Component	To ensure that an entity is the person or application that claims the identity provided
Access Control	HITSP/TP20	Transaction Package	To ensure that an entity can access protected resources if they are permitted to do so
Nonrepudiation of Origin	HITSP/C26	Component	To support Nonrepudiation of Origin
Manage Consent Directives	HITSP/TP30	Transaction Package	To ensure that a consumer's consent directive relating to the collection, access, use, or disclosure of the consumer's IIHI are captured, managed and available to requesting actors, e.g., a Document Source deploying the consent directive in the course of collecting, publishing, and registering the IIHI



# Base and Composite Standards

---

- ▶ Per HITSP definition the term “standard” refers, but is not limited to:
  - Basic Specifications
  - Implementation Guides
  - Code Sets
  - Terminologies
  - Integration Profiles
- ▶ A base standard is capable of fulfilling a discrete function within a single category produced and maintained by a single standards organization
- ▶ Composite standards are groupings of coordinated base standards, often from multiple standards organizations, maintained by a single organization.



# Security & Privacy Selected Standards

---

- ▶ Originally 249 candidate standards (including reference documents/guidelines) identified in the RDSS as candidates to meet the security requirements from the EHR-Lab, Consumer Empowerment and Biosurveillance 2006 Use Cases.
- ▶ Final selection:
  - 8 Composite Standards
  - 20 Base Standards
- ▶ Final Selection includes some standards previously selected and that had already been incorporated into HITSP IS-01, IS-02, IS-03



# Security & Privacy Selected Standards

---

## Selected Composite Standards:

IHE XUA  
IHE BPPC  
IHE ATNA  
IHE Consistent Time  
IHE DSG  
IHE XDS (ITI-14/15/16/17)  
IHE XDS.B (via TP13)  
IHE NAV

## Selected Base Standards:

ASTM E2147  
ASTM E1762-2005  
DICOM Supplement 95  
HL7 Data Consent Message  
HL7 Confidentiality Codes  
HL7 v3.0 Consent Related Vocabulary  
ISO 10164-7  
ISO 15000 ebRS  
ITU-T X.509  
OASIS SAML 2.0  
OASIS WS-Security  
OASIS WS-Federation  
OASIS WS-Trust  
OASIS XACML  
RFC 3881 (Healthcare Audit Log)  
RFC 1305 (NTP)  
RFC 2030 (SNTP)  
RFC 2246 (TLS)  
RFC 3164 –BSD Syslog  
W3C XML Digital Signature



# Future Use Cases

---

## ▶ 2008 Use Cases with Security and Privacy implications

- Remote Consultation
- Remote Monitoring
- Immunizations & Response Management
- Personalized Healthcare
- Public Health Case Reporting
- Consultation and Transfers of Care

## ▶ 2009 and Beyond Use Cases for Security and Privacy

- CC 18.0 Patient identification for authorization and authentication
- AHIC 2.0 Secure messaging/online consultation
- AHIC 7.0 Identification/authentication
- AHIC 14.0 Confidentiality, privacy, & security of patient data
- AHIC 15.0 Data access/data control
- AHIC 17.1 Security, network, repositories
- AHIC 30.0 Provider list
- HITSP 5.0 Cross use case work on security (standards)
- HITSP 5.3 Authentication models to support chain of trust data exchanges
- AHIC 46.0 Legal liability & regulatory barriers
- AHIC 47.0 Consumer consent

